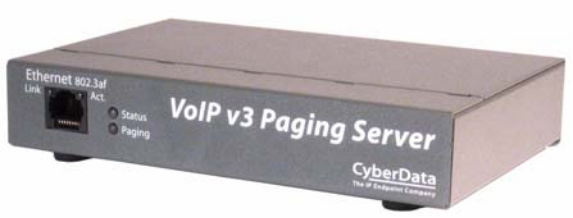
CyberData

The IP Endpoint Company



VoIP V3 Paging Server Operations Guide

SIP Compliant

Part #*011146*

Document Part #*930427I*
for Firmware Version 7.0.0

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

Operations Guide 930427I
SIP Compliant 011146

COPYRIGHT NOTICE:
© 2013, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by Cyberdata that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://www.cyberdata.net/support/contactsupportvoip.php

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

Revision 930427I, which corresponds to firmware version 7.0.0, was released on August 29, 2013, and has the following changes:

- Updates the description for the Beep on Page setting in Table 2-6, "Device Configuration Parameters".

Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Pictorial Alert Icons

GENERAL ALERT	**General Alert** This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.
	Ground This pictoral alert indicates the Earth grounding connection point.

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Abbreviations and Terms

Abbreviation or Term	Definition
A-law	A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.
AVP	Audio Video Profile
Cat 5	TIA/EIA-568-B Category 5
DHCP	Dynamic Host Configuration Protocol
LAN	Local Area Network
LED	Light Emitting Diode
Mbps	Megabits per second.
NTP	Network Time Protocol
PBX	Private Branch Exchange
PoE	Power over Ethernet (as per IEEE 802.3af standard)
RTFM	Reset Test Function Management
SIP	Session Initiated Protocol
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

Chapter 1 Product Overview 1

1.1 How to Identify This Product 2
1.2 Product features 3
1.3 Product Specifications 4

Chapter 2 Setting Up the V3 Paging Server 5

2.1 Parts List 5
2.2 Typical Installation 6
2.3 Connecting the V3 Paging Server 7
2.3.1 Connection Options 7
Pin 1 and 2—Fault Sense Input (Common/Sense) 8
Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference 8
Pin 6 and 7—Relay Contact (Common/Normally Open) 8
2.3.2 Removable Connector 8
2.3.3 Connect to the Power Source 9
Poe 9
Non-Poe 9
Chassis Ground 9
2.3.4 Connect to the Network 10
2.3.5 Confirm that the V3 Paging Server is Up and Running 11
Confirm Power on, Network Connectivity, and Connection Speed 11
Verify Network Activity 11
2.3.6 Announcing the IP Address 12
2.3.7 Restore the Factory Default Settings 12
2.4 Configuring the V3 Paging Server 13
2.4.1 Gather the Required Configuration Information 13
Static or DHCP Addressing? 13
Username and Password for Configuration GUI 13
SIP Settings 13
2.4.2 V3 Paging Server Web Page Navigation 14
2.4.3 Log in to the Configuration GUI 15
2.4.4 Configure the Device Parameters 19
2.4.5 Configure the Network Parameters 22
2.4.6 Configure the SIP Parameters 25
Point-to-Point Configuration 28
2.4.7 Configure the Night Ringer Parameters 29
2.4.8 Configure the Fault Detection Parameters 31
2.4.9 Configure the Paging Groups (PGROUPS) Parameters 33
2.4.10 Operating the Paging Server 42
DTMF Bypassed 42
DTMF Not Bypassed 42
2.4.11 Configure the Audio Parameters 43
User-created Audio Files 48
2.4.12 Configure the Event Parameters 51
Example Packets for Events 53
2.4.13 Configure the Autoprovisioning Parameters 56
Autoprovisioning 58
Get Autoprovisioning Template Button 61
Time Zone Strings 62
2.5 Upgrading the Firmware 65
2.5.1 Uploading the Firmware 66

Upgrade the Firmware 67
2.5.2 Reboot the V3 Paging Server 68
2.6.1 Command Interface Post Commands 69

Appendix A Setting Up a TFTP Server 73
A.1 Set up a TFTP Server 73
A.1.1 In a LINUX Environment 73
A.1.2 In a Windows Environment 73

Appendix B Troubleshooting/Technical Support 74
B.1 Frequently Asked Questions (FAQ) 74
B.1.1 Documentation 74
B.2 Contact Information 75
B.3 Warranty 76
B.3.1 Warranty & RMA Returns within the United States 76
B.3.2 Warranty & RMA Returns outside of the United States 76
B.3.3 Spare in the Air Policy 77
B.3.4 Return and Restocking Policy 77
B.3.5 Warranty and RMA Returns Page 77

1 Product Overview

The CyberData V3 VoIP Paging Server enables users through a single SIP phone extension, to access multiple zones for paging in a VoIP network and to connect to legacy analog overhead paging systems.

A second SIP extension can be configured as a night ringer playing a user-uploadable audio file.

The V3 Paging Server allows direct connection to legacy analog paging amplifiers that require a "Page Port" type of input that meets a balanced 600 Ohm 10Vpp signal or a 10k Ohm Hi-Z 2vpp signal. You can also take advantage of connections for a dry contact relay (page start output) and sense input (Fault Sense Input) for additional functionality.

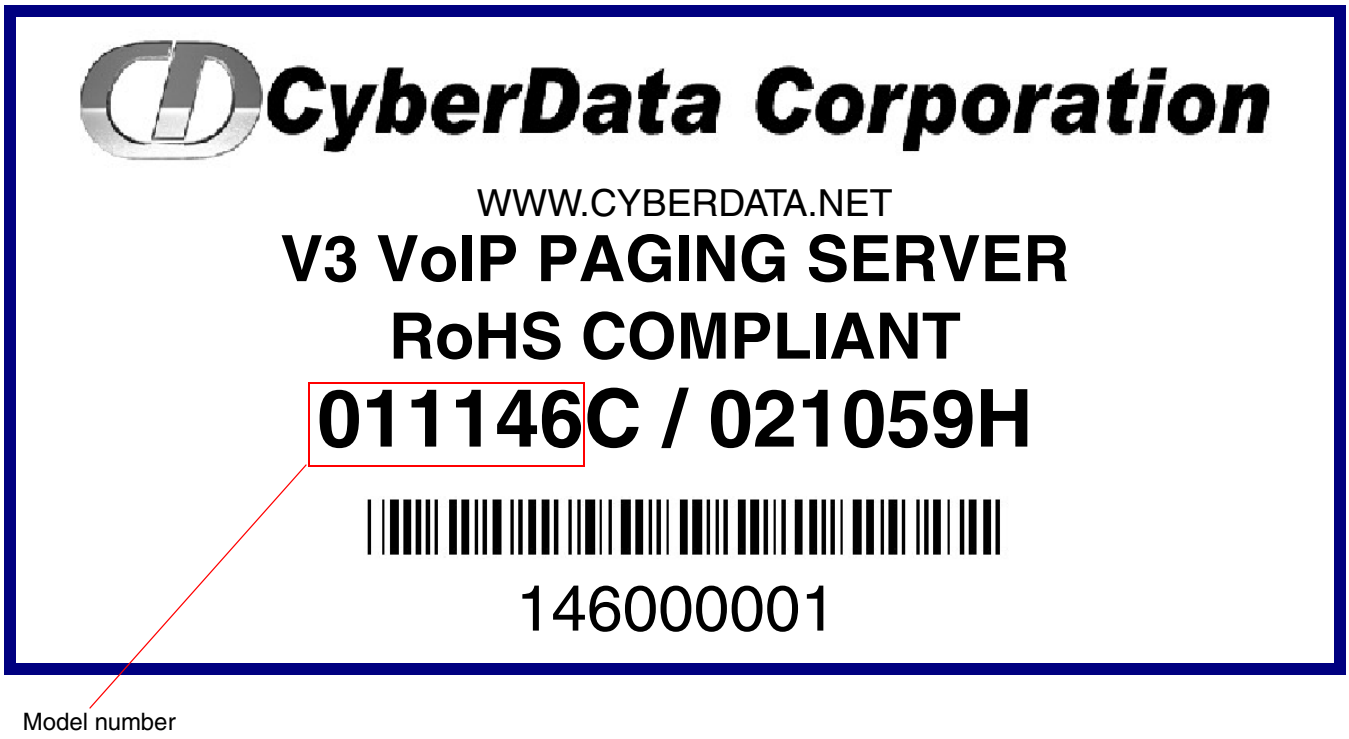
The easy-to-use, web-based configuration provides a graphical user interface to set up to 100 paging zones for IP paging with unique multicast address and port number combinations.

The V3 Paging Server connects via a single CAT 5 or 6 network cable to a standard PoE 802.3af compliant switch.

1.1 How to Identify This Product

To identify the VoIP V3 Paging Server, look for a model number label similar to the one shown in Figure 1-1. The model number on the label should be **011146**.

Figure 1-1. Model Number Label



1.2 Product features

- SIP RFC 3261
- Two SIP endpoints (one for Night Ringer)
- Multicast output
- DTMF control of zone selection (with optional security code per zone)
- RTP Version 2 Multicast and Unicast
- Delayed page support
- Line-In connection for music-on-hold multicasting
- Line-out connection to support analog Amps
- Audio Codecs
  - G.711 U-law
  - G.711 A-law
  - Speex
  - DTMF detection (via RFC 2833)
- Cisco SRST support
- 802.11Q VLAN support
- Ability to import and export configuration
- Auto Provisioning
- Added support for NTP server for time keeping
  - TFTP or HTTP
  - Update at certain times of day
  - Update after a certain amount of idle time
- HTTP command interface
- Remote amp fault sensor
- Web-based configuration and firmware upload
- User uploadable audio files
- PoE 802.3af enabled (Power-over-Ethernet)
- 19-inch Rack mount option

1.3 Product Specifications

Table 1-1. Product Specifications

Specifications	
Regulatory Compliance	FCC Class A, UL 60950, CE
Power Requirement	PoE or 48V DC
Connection Speed	10/100 Mbps
Protocol	SIP compliant
Page Port Output	Balanced 600 Ohm 10VPP
Line In:	
Input Signal Amplitudes	2.0 VPP maximum
Input Impedance	10k Ohm
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
Part Number	011146
Dimensions	6.11” L x 4.05” W x 1.15” H
Weight	1.2 pounds

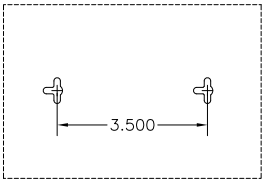
2 Setting Up the V3 Paging Server

The topics in this chapter provide information on setting up, configuring, and using the VoIP V3 Paging Server.

2.1 Parts List

The packaging for the V3 Paging Server includes the parts in Table 2-2.

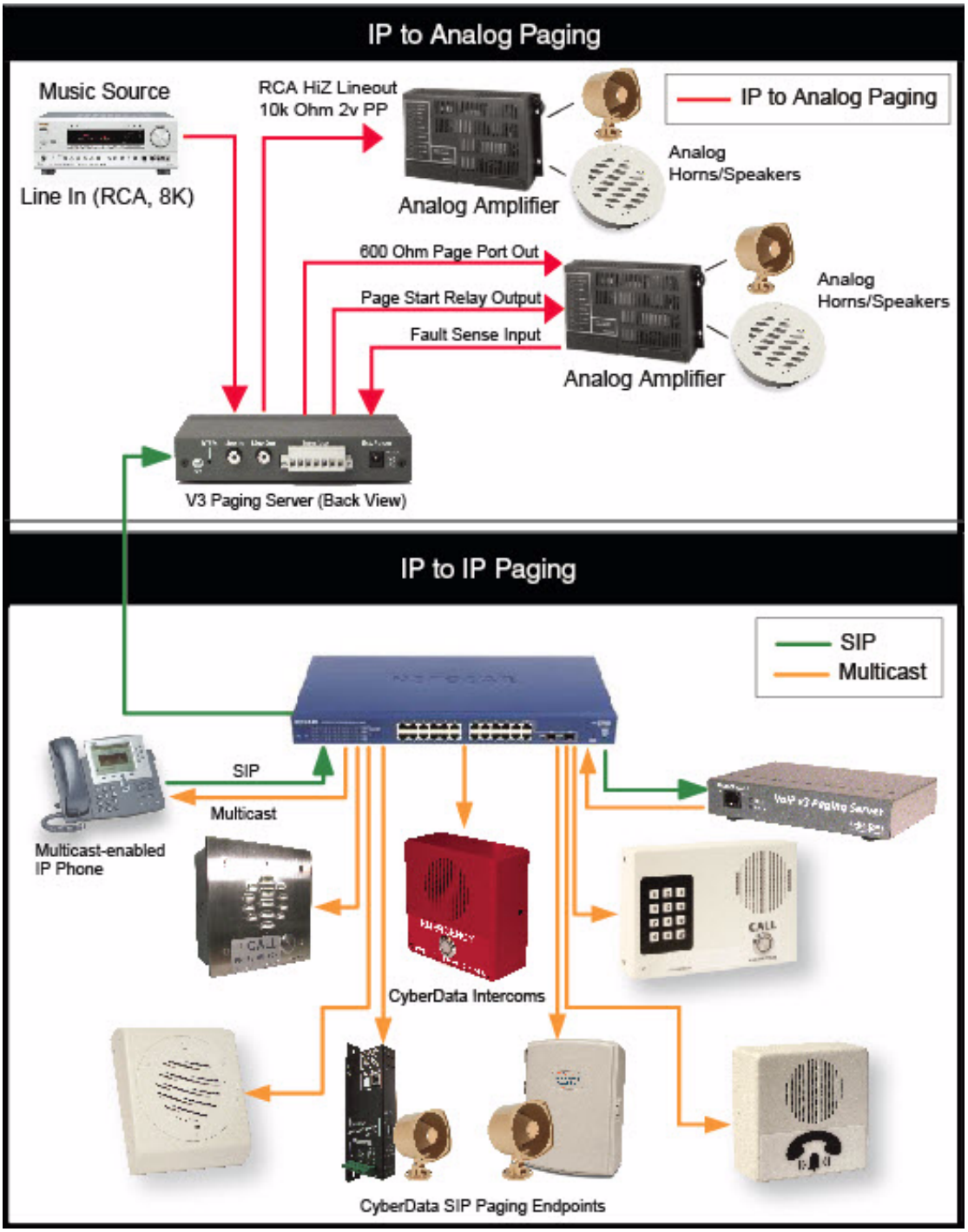
Table 2-2. Parts List

Quantity	Part Name	Illustration
1	V3 Paging Server	
1	Installation Quick Reference Guide	
1	Mounting Template (located on the last page of the *Installation Quick Reference*)	
1	Mounting Kit (part #070057A) which includes: (2) #4-6 x 7/8" Mounting Anchors (2) #4 x 1-1/4" Round Phillips Wood Screws	

2.2 Typical Installation

Figure 2-2 illustrates how the V3 Paging Server is normally installed as part of a paging system.

Figure 2-2. Typical Installation



2.3 Connecting the V3 Paging Server

Before you connect the V3 Paging Server, be sure that you have received all of the parts described in Section 2.1, "Parts List".

2.3.1 Connection Options

See Figure 2-3 and Table 2-1 for the connection options that are available for the V3 Paging Server.

Figure 2-3. Connection Options

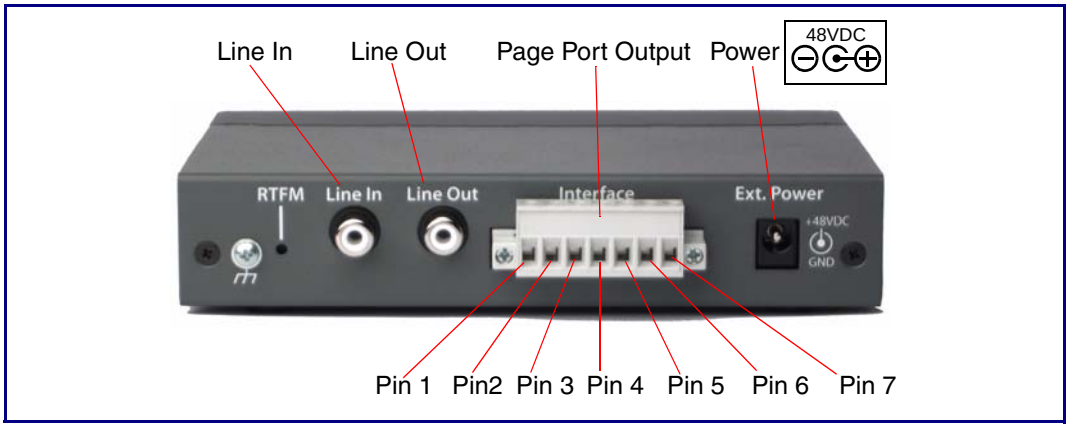


Table 2-1. Page Port Output Connections

Pin	Description
1	Fault Sense Input (Common). See Section 2.3.1.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)".
2	Fault Sense Input (Sense). See Section 2.3.1.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)".
3	Positive 600-Ohm Audio Output[a]. See Section 2.3.1.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
4	Negative 600-Ohm Audio Output.[a]. See Section 2.3.1.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
5	Audio Ground Reference. See Section 2.3.1.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
6	Relay Contact - Common[b]. See Section 2.3.1.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)".
7	Relay Contact - Normally Open[b]. See Section 2.3.1.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)".

a. The 600-Ohm audio output of the page port is also suited for interfaces with lower input impedances.
b. 1 Amp at 30 VDC for continuous loads

2.3.1.1 Pin 1 and 2—Fault Sense Input (Common/Sense)

This input was designed as a method of monitoring an external amplifier that is equipped with a fault sense relay.

When enabled via the web interface (Section 2.4.8, "Configure the Fault Detection Parameters"), this input (when closed) will play a user uploadable audio file out of the line-out connection and/or place a SIP call to a pre-determined extension and play that file.

2.3.1.2 Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference

This output allows direct connection to paging amplifiers requiring a "Page Port" type input that meets a balanced 600 Ohm 10Vpp signal.

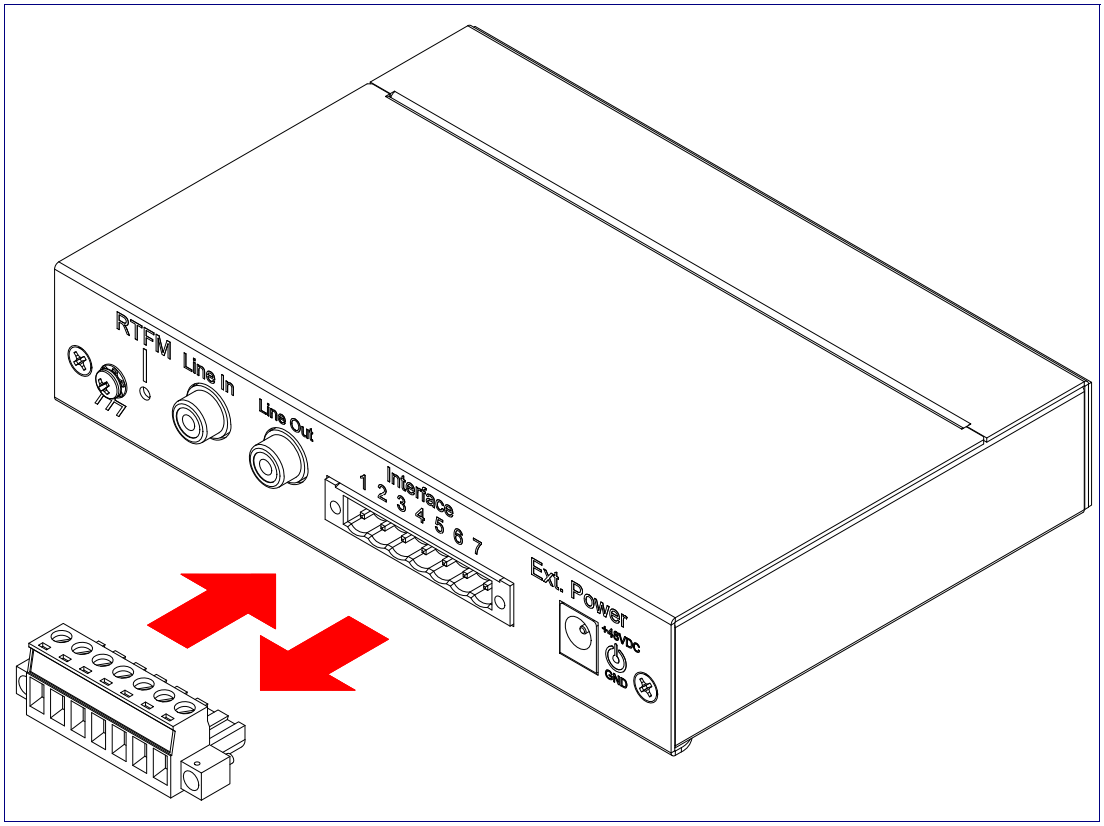
2.3.1.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

When enabled on the web interface (Section 2.4.4, "Configure the Device Parameters"), every time an audio file is played out of the local line-out or 600 Ohm output, the relay will close, thereby enabling amplifiers with a remote turn-on capability to become active.

2.3.2 Removable Connector

Figure 2-4 shows the connector that is removable on the V3 Paging Server.

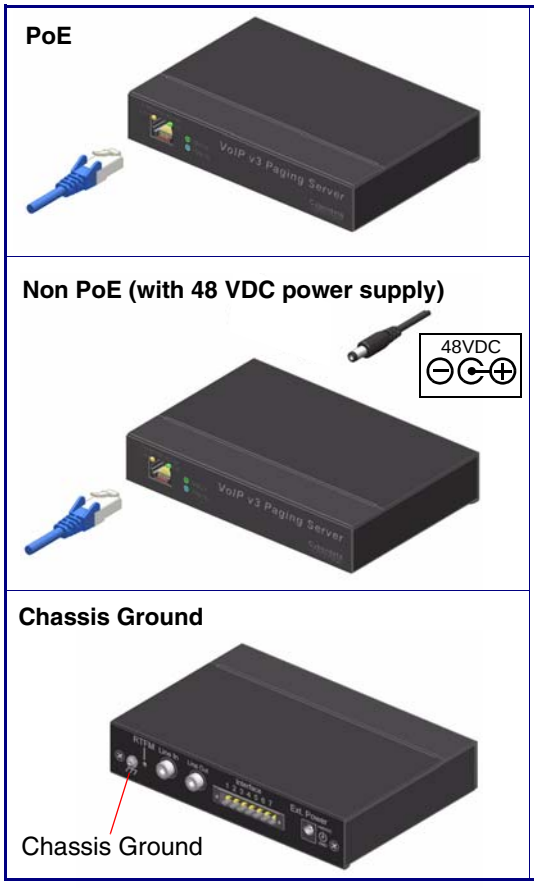
Figure 2-4. Removable Connector



2.3.3 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the V3 Paging Server **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the Paging Server, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit. See Figure 2-5.

Figure 2-5. Connecting to the Power Source



To set up the V3 Paging Server, connect the device to your network:

Poe

- For **PoE**, plug one end of an 802.3af Ethernet cable into the V3 Paging Server Ethernet port. Plug the other end of the Ethernet cable into your network. See the figure on the left.

Non-Poe

- For **Non-PoE**, connect the V3 Paging Server to a **48VDC power supply**. See the figure on the left.

Chassis Ground

- If required, connect the earth grounding wire to the **Chassis Ground**. See the figure on the left.

2.3.4 Connect to the Network

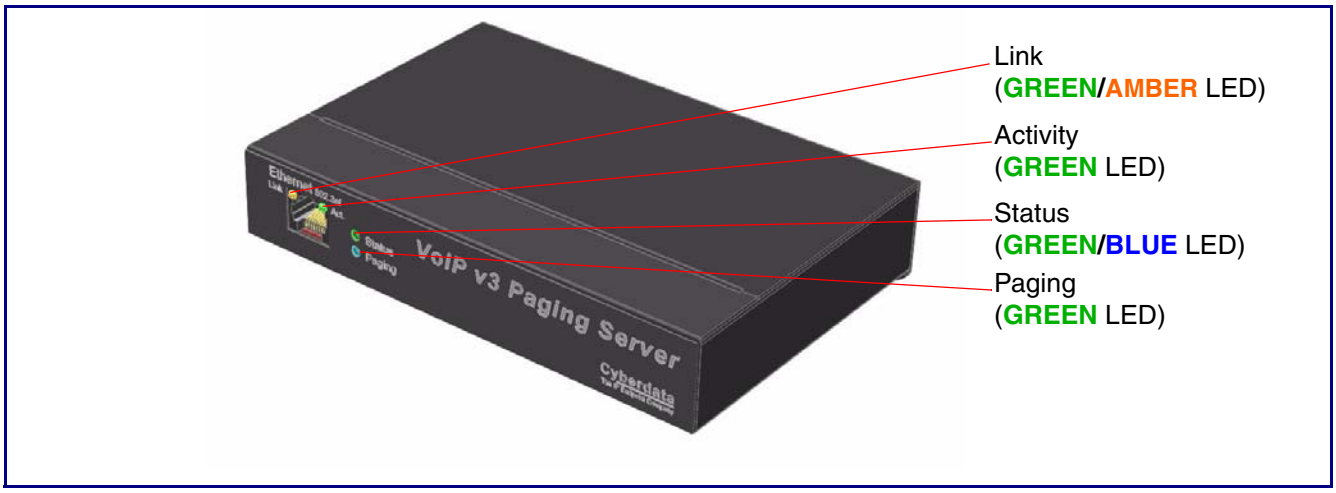
Plug one end of a standard Ethernet cable into the Paging Server **Ethernet** port. Plug the other end into your network.

Figure 2-6. Connecting to the Network

2.3.5 Confirm that the V3 Paging Server is Up and Running

The LEDs on the front of the V3 Paging Server verify the unit's operations.

Figure 2-7. Paging Server LEDs



2.3.5.1 Confirm Power on, Network Connectivity, and Connection Speed

When you plug in the Ethernet cable or power supply:

- The **GREEN/BLUE Status** LED and the **GREEN Paging** LED both blink at a rate of 10 times per second during the initial network setup.
- The round, **GREEN/BLUE Status** LED on the front of the V3 Paging Server comes on indicating that the power is on. Once the device has been initialized, this LED blinks at one second intervals.
- The square, **GREEN/AMBER Link** LED above the Ethernet port indicates that the network connection has been established. The Link LED changes color to confirm the auto-negotiated connection speed:
  - The Link LED is **GREEN** at 10 Mbps.
  - The Link LED is **AMBER** at 100 Mbps.
- The **GREEN Paging** LED comes on after the device is booted and initialized. This LED blinks when a page is in progress. You can disable **Beep on Initialization** on the **Device Configuration** page.

2.3.5.2 Verify Network Activity

The square, **GREEN Activity** LED blinks when there is network traffic.

2.3.6 Announcing the IP Address

To announce the IP address for the V3 Paging Server, briefly press and then quickly release the RTFM switch. See Figure 2-8.

Figure 2-8. RTFM Switch

2.3.7 Restore the Factory Default Settings

The V3 Paging Server is delivered with factory set default values for the parameters in Table 2-3. Use the RTFM switch (see Figure 2-8) on the back of the unit to restore these parameters to the factory default settings.

Note When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in Table 2-3.

Table 2-3. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

a. Default if there is not a DHCP server present.

To restore these parameters to the factory default settings:

1. Press and hold the RTFM switch until the status and paging lights come on.
2. Continue to press the RTFM switch until after you see the indicator lights go off and you hear the “restoring defaults” announcement.
3. Release the RTFM switch.
4. The V3 Paging Server settings are restored to the factory defaults.

2.4 Configuring the V3 Paging Server

Use this section to configure the VoIP paging server.

2.4.1 Gather the Required Configuration Information

Have the following information available before you configure the V3 Paging Server.

2.4.1.1 Static or DHCP Addressing?

Know whether your system uses static or dynamic (DHCP) IP addressing. If it uses static addressing, you also need to know the values to assign to the following V3 Paging Server parameters:

- IP Address
- Subnet Mask
- Default Gateway

2.4.1.2 Username and Password for Configuration GUI

Determine the Username and Password that will replace the defaults after you initially log in to the configuration GUI.

- The Username is case-sensitive, and must be from four to 25 alphanumeric characters long.
- The Password is case-sensitive, and must be from four to 20 alphanumeric characters long.

2.4.1.3 SIP Settings

To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values for these parameters:

- SIP Server IP Address
- Remote and Local SIP Port Numbers
- SIP User ID, and Authenticate ID and Password for this User ID

2.4.2 V3 Paging Server Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every V3 Paging Server web page.

Table 2-4. V3 Paging Amplifier Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device Configuration** page.
	Link to the **Networking** page.
	Link to go to the **SIP Configuration** page.
	Link to go to the **Nightringer** page.
	Link to go to the **Fault Detection** page.
	Link to go to the **Paging Groups Configuration** page.
	Link to the **Audio Configuration** page.
	Link to the **Event Configuration** page.
	Link to the **Autoprovisioning Configuration** page.
	Link to the **Upgrade Firmware** page.

2.4.3 Log in to the Configuration GUI

1. Open your browser to the V3 Paging Server IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the V3 Paging Server.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

http://www.cyberdata.net/support/voip/discovery_utility.html

The unit ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

Note To work with the V3 Paging Server configuration *after* the initial configuration, log in using the IP address you assign to the device. Section 2.4.5, "Configure the Network Parameters" provides instructions for entering the IP address.

2. When prompted, use the following default **Username** and **Password** to open the configuration Home page:

   Username: **admin**

   Password: **admin**

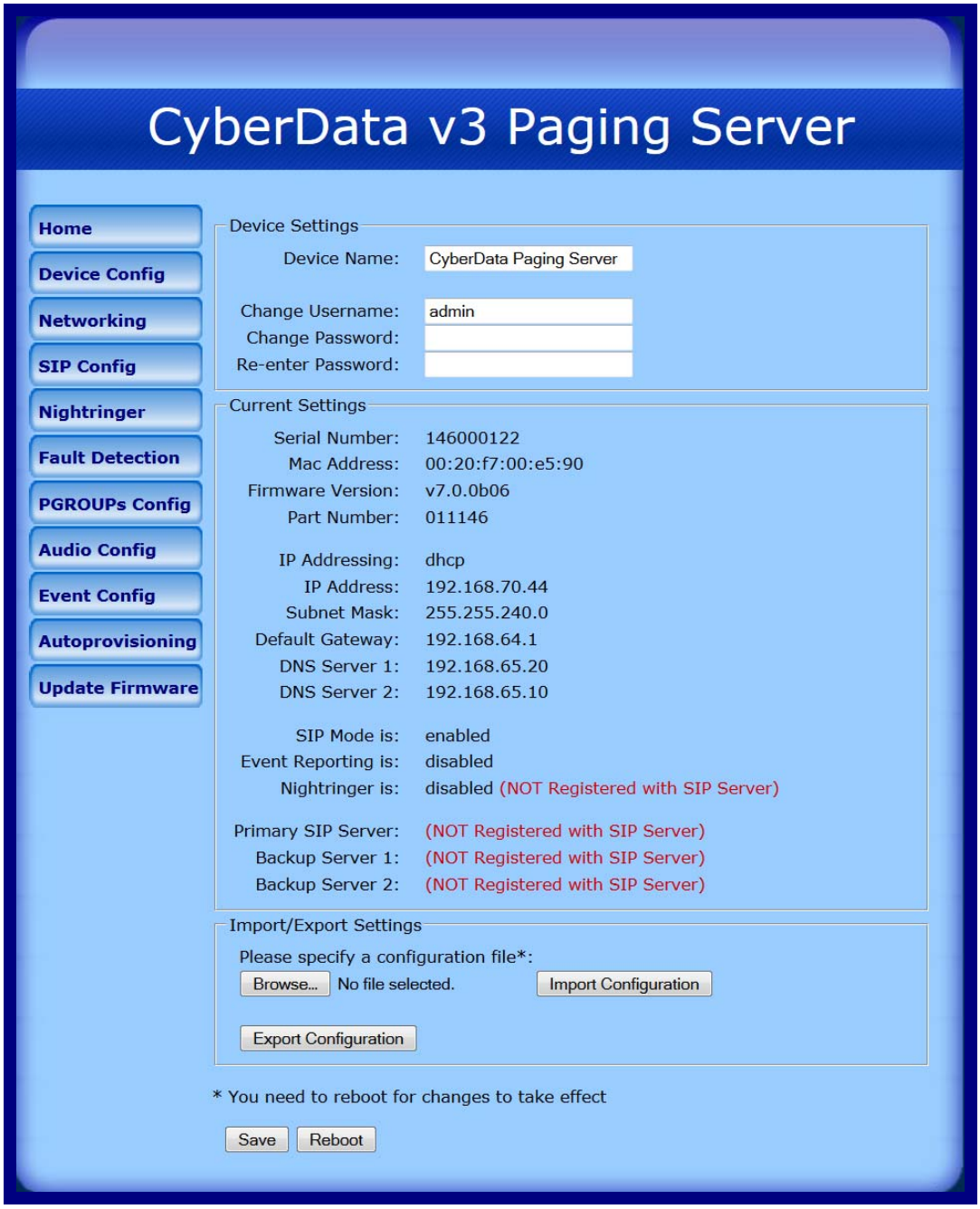
Change the Default Username and Password

To change the default Web access Username and Password:

1. Enter the new Username from four to 25 alphanumeric characters in the **Change Username** field. The Username is case-sensitive.
2. Enter the new Password from four to 20 alphanumeric characters in the **Change Password** field. The Password is case-sensitive.
3. Enter the new password again in the **Re-enter New Password** field.

   Click **Save Settings**.

Figure 2-9. Home Page



4. On the **Home Page**, review the setup details and navigation buttons described in Table 2-5.

Table 2-5. Home Page Overview

Web Page Item	Description
Device Settings	
Device Name	Shows the device name (25 character limit).
Change Username	Type in this field to change the username (25 character limit).
Change Password	Type in this field to change the password (20 character limit).
Re-enter Password	Type the password again in this field to confirm the new password (20 character limit).
Current Settings	
Serial Number	Shows the serial number of the device.
Part Number	Shows the part number of the device.
Mac Address	Shows the Mac address of the device.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **Static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode is	Shows the current status of the SIP Mode.
Event Reporting is	Shows the current status of the Event Reporting.
Nightring is	Shows the current status of the Nightringer.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Import/Export Settings	The user can export and edit the device's configuration (in XML format), and then reload it to a device (or devices) instead of making changes through the web interface.
Browse...	Press the **Browse** button to select a configuration file to import.
Import Configuration	IPress the **Import Configuration** button to save a board configuration to the board. **Note**: The board will have to be reset before changes will take effect.
Export Configuration	Press the **Export Configuration** button to download the current board configuration.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

At this point you can:

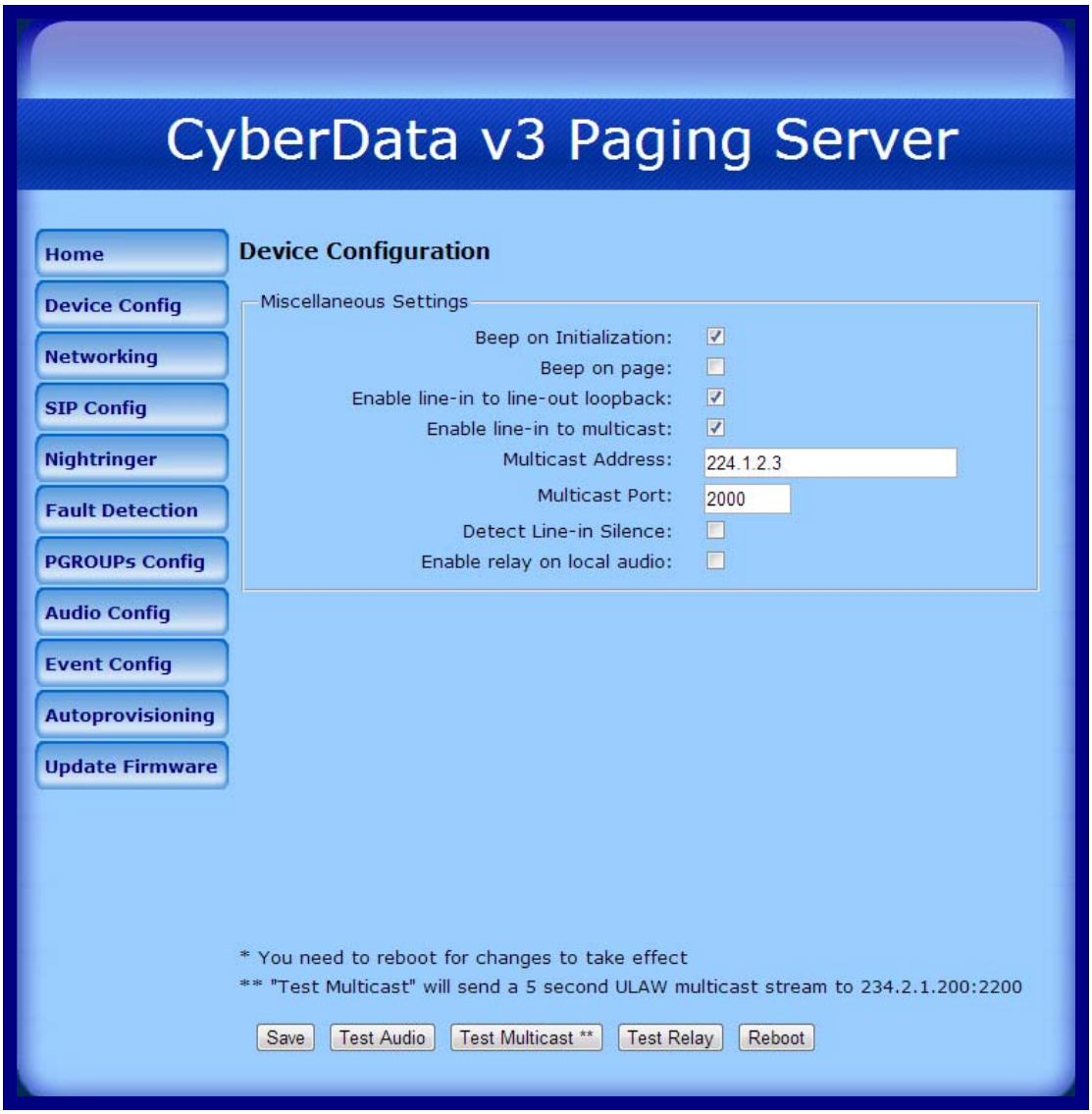
- Review the V3 Paging Server's **Current Settings**. Use the RTFM switch to restore the factory default settings. See Section 2.3.7, "Restore the Factory Default Settings".
- Configure the device parameters. Click on the **Device Config** button and see Section 2.4.4, "Configure the Device Parameters".
- Configure the network parameters. Click on the **Networking** button and refer to Section 2.4.5, "Configure the Network Parameters" for instructions.
- Configure the SIP parameters. Click on the **SIP Config** button and see Section 2.4.6, "Configure the SIP Parameters".
- Configure the Night Ringer parameters. Click on the **Nightringer** button and see Section 2.4.7, "Configure the Night Ringer Parameters".
- Configure the fault detection parameters. Click on the **Fault Detection** button and see Section 2.4.8, "Configure the Fault Detection Parameters".
- Configure the PGROUPS parameters. Click on the **PGROUPS Config** button and see Section 2.4.9, "Configure the Paging Groups (PGROUPS) Parameters" for instructions.
- Configure the audio parameters. Click on the **Audio Config** button and see Section 2.4.11, "Configure the Audio Parameters" for instructions.
- Configure the event parameters. Click on the **Event Config** button and see Section 2.4.12, "Configure the Event Parameters" for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprovisioning** button and see Section 2.4.13, "Configure the Autoprovisioning Parameters" for instructions.

Note Click on the **Update Firmware** button any time you need to upload new versions of the firmware. See Section 2.5, "Upgrading the Firmware" for instructions.

2.4.4 Configure the Device Parameters

1. Click on the **Device Configuration** button to open the **Device Configuration** page. See Figure 2-10.

Figure 2-10. Device Configuration Page



2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-6.

Table 2-6. Device Configuration Parameters

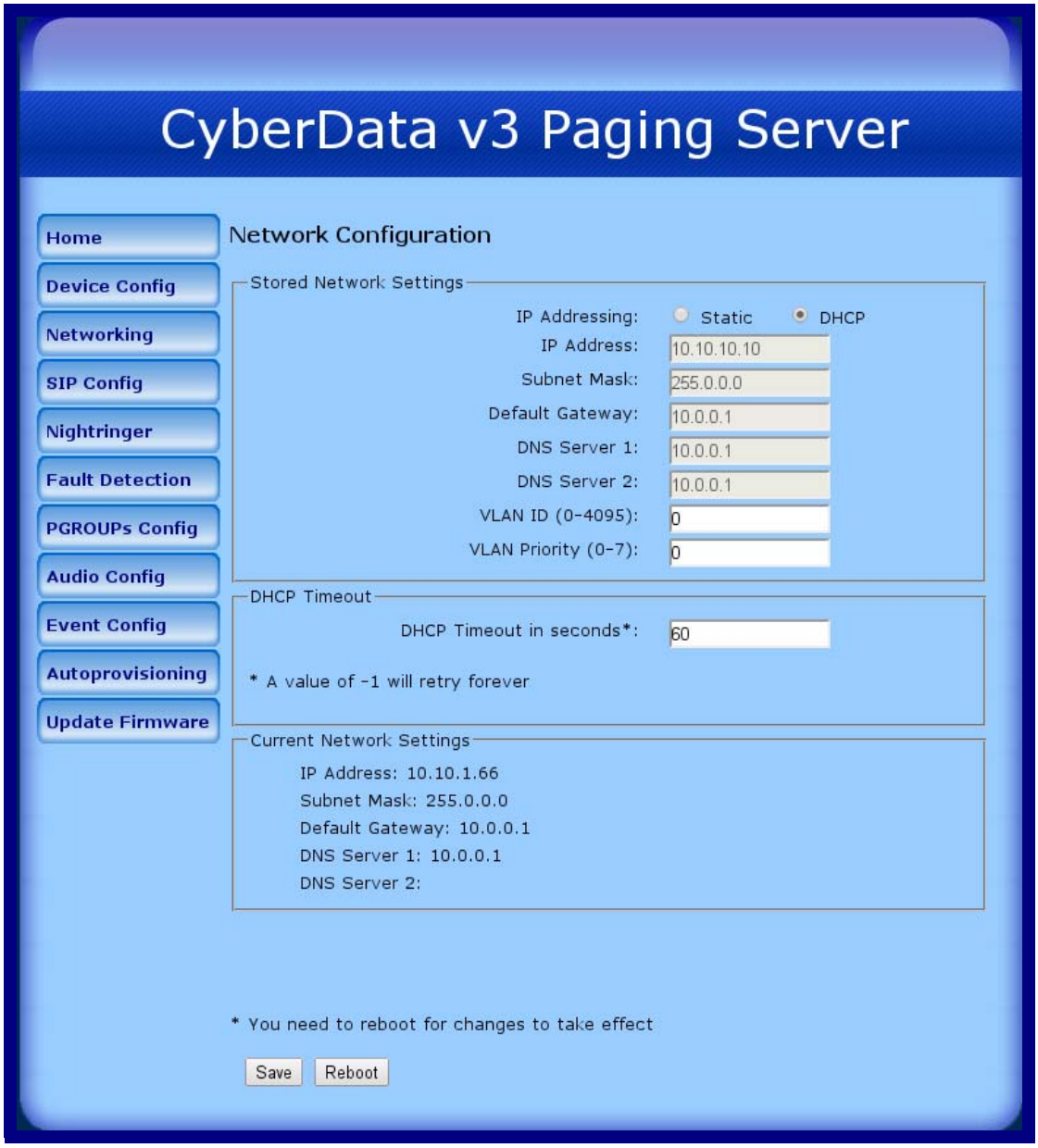
Web Page Item	Description
Miscellaneous Settings	
Beep on Initialization	When selected, you will hear a beep when the device initializes.
Beep on Page	When selected, the device will play a beep before a page is sent to the analog ports when "Lineout" is enabled on a paging group (works for both buffered and live pages).
Enable Line In to Line Out Loopback	When selected, audio is sent from the line -in to the line-out output.
Enable Line-In to Multicast	When selected, the line-in audio will be multicast to the address and port specified on the web page. **Note**: Ideally, the specified address and port will match that of a low priority MGROUP (such as background music) on the speakers or paging amplifiers. **Note**: When line-in to multicast is selected, do not set that multicast address and port to the same multicast address and port that is used by one of your PGROUPS. Otherwise, when you call the PGROUP, the Paging Server will be unable to send the new audio stream because the port will already be in use by the line-in to multicast stream.
Multicast Address	Type the Multicast address.
Multicast Port	Type the Multicast port number.
Detect Line-in Silence	When selected, the device will detect when silence occurs in the line-in port. Also, the device will not relay line-in audio to multicast if this option is enabled and there is silence on the line-in port. **Note**: This option requires a 011146C/021059G/991034C or newer Paging Server.
Enable Relay on Local Audio	When selected, the relay will be closed any time that audio is played out of the line-out/page port. This setting is for legacy analog amplifiers that are often connected to the page port. Analog amplifiers will often have a noticeable hum if they are turned on while there is no audio being played. The relay closure causes these amplifiers to turn on only when audio is sent to them.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Audio	When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
Test Multicast **	When the **Test Multicast** button is pressed, the Paging Server will send a five second canned ULAW message to a predetermined multicast address and port.
Test Relay	Click on the **Test Relay** button to do a relay test.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.4.5 Configure the Network Parameters

Configuring the network parameters enables your network to recognize the V3 Paging Server and communicate with it. Click the **Networking** button on the **Home** page to open the **Network Configuration** page.

Figure 2-11. Network Configuration Page



On the **Network Configuration** page, enter values for the parameters indicated in Table 2-7.

Table 2-7. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	Shows the settings stored in non-volatile memory.
IP Addressing	Select either **DHCP IP Addressing** or **Static IP Addressing** by marking the appropriate radio button. If you select **Static**, configure the remaining parameters indicated in Table 2-7. If you select **DHCP**, go to Step 3.
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
VLAN ID (0-4095)	Enter the VLAN ID number. **Note**: The device supports 802.11Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7)	Enter the VLAN priority number.
DHCP Timeout	
DHCP Timeout in seconds	Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address. **Note**: A value of **-1** will cause the device to retry indefinitely and a value of **0** will cause the device to reset to a default of 60 seconds.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

On this page:

1. Specify whether you use **Static** or **DHCP IP Addressing** by marking the appropriate radio button. If you select **Static IP Addressing**, go to Step 2.
2. For Static IP Addressing, also enter values for the following parameters:
   - The V3 Paging Server’s **IP Address**: The V3 Paging Server is delivered with a factory default IP address. Change the default address to the correct IP address for your system.

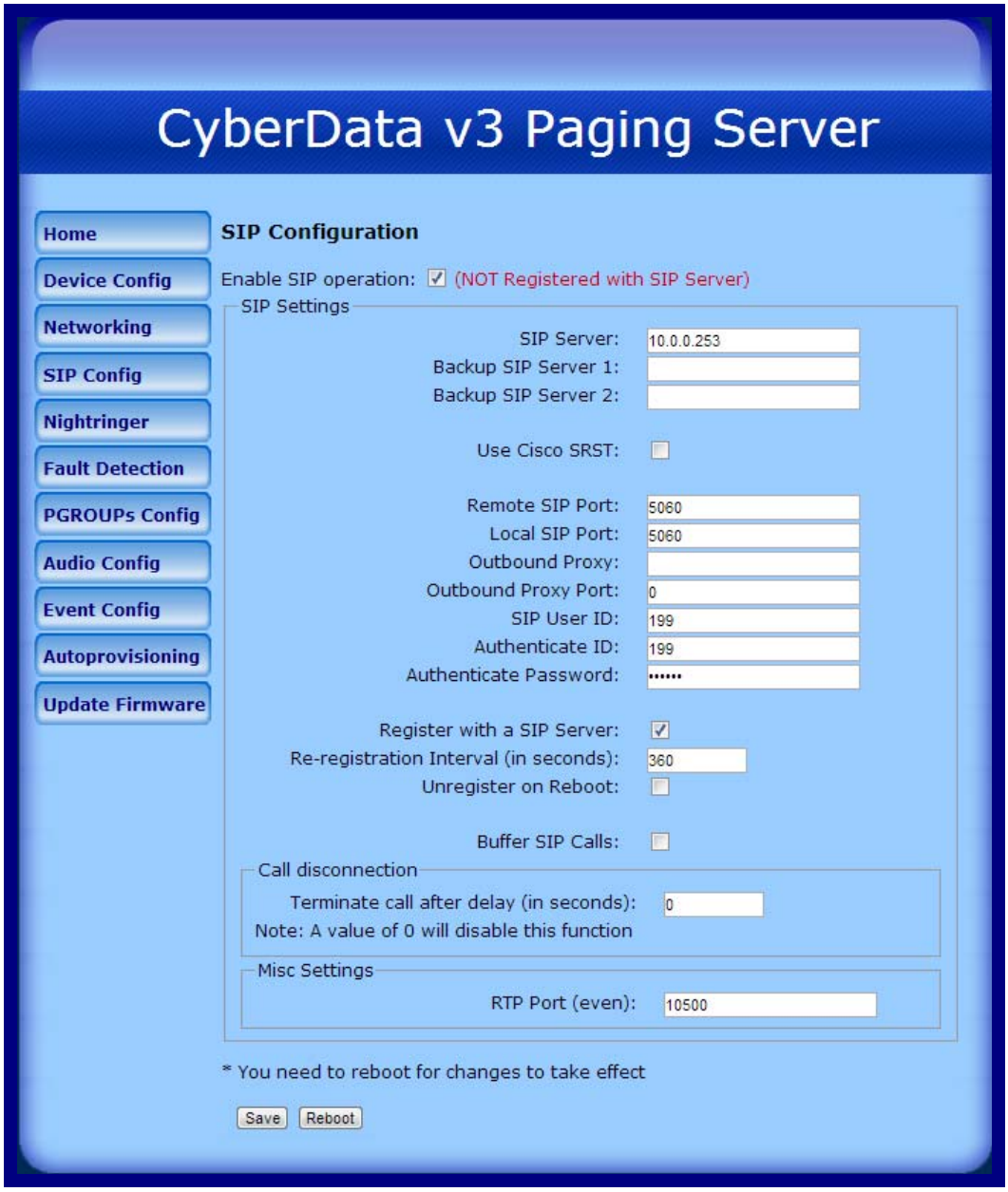
- The **Subnet Mask.**
- The **Default Gateway.**

3. Click **Save** when you are finished.
4. Click **Reboot** for the new settings to take effect.

2.4.6 Configure the SIP Parameters

The SIP parameters enable the V3 Paging Server to contact and register with the SIP server. On the Home page, click **SIP Config** to open the **SIP Configuration** page.

Figure 2-12. SIP Configuration Page



5. On the **SIP Configuration** page, enter values for the parameters indicated in Table 2-8.

Table 2-8. SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
SIP Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Backup SIP Server 1 Backup SIP Server 2	• If all of the **SIP Server** and **Backup SIP Server** fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the **Backup SIP Server 1** and **Backup SIP Server 2** fields blank if they are not needed. • In the event of a registration failure on the **Primary SIP Server**, the device will use the next highest priority server for outbound calls (**Backup SIP Server 1**). If **Backup SIP Server 1** fails, the device will use **Backup SIP Server 2**. • If a higher priority SIP Server comes back online, the device will switch back to this server.
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port	Type the **Remote SIP Port** number (default 5060) (5 character limit [values from 1 to 65535]).
Local SIP Port	Type the **Local SIP Port** number (default 5060) (5 character limit [values from 2000 to 65535]).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (5 character limit [values from 1 to 65535]).
SIP User ID	Type the **SIP User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Register with a SIP Server	Enable or disable SIP Registration. For information about Point-to-Point Configuration, see Section 2.4.6.1, "Point-to-Point Configuration".
Re-registration Interval (in seconds)	Type the SIP Registration lease time in seconds (default is 60 minutes) (4 character limit [values from 30 to 3600]). Re-registration Interval (in seconds)
Unregister on Reboot	When selected, on boot, the device will first register with a SIP server with a expiration delay of 0 seconds. This has the effect of unregistering any current devices on this extension.

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
Buffer SIP Calls	When this is enabled, SIP calls to the device will be stored in memory and will play when either the call is terminated or the buffer is full. The receive buffer is 2MB in size and this is equal to about four minutes of ulaw encoded audio.
Call Disconnection	
Terminate call after delay (in seconds)	Type the desired number of seconds that you want to transpire after a connection delay before a call is terminated. Note: A value of **0** will disable this function.
Misc Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500 (values from 2000 to 65534).
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

1. Enter the IP address of the **SIP Server**.
2. Enter the port numbers used for SIP signaling:
   a. **Remote SIP Port**
   b. **Local SIP Port**
3. Enter the SIP registration parameters:
   a. **SIP User ID**
   b. **Authenticate ID**
   c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the VoIP Paging Server to register with your SIP server.
5. At **Unregister on Reboot**:
   a. Select **Yes** to automatically unregister the V3 Paging Server when you reboot it.
   b. Select **No** to keep the V3 Paging Server registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the V3 Paging Server registration lease remains valid with the SIP Server. The V3 Paging Server automatically re-registers with the SIP server before the lease expiration timeout.
7. Click **Save**.
8. Click **Reboot** for the new settings to take effect.

2.4.6.1 Point-to-Point Configuration

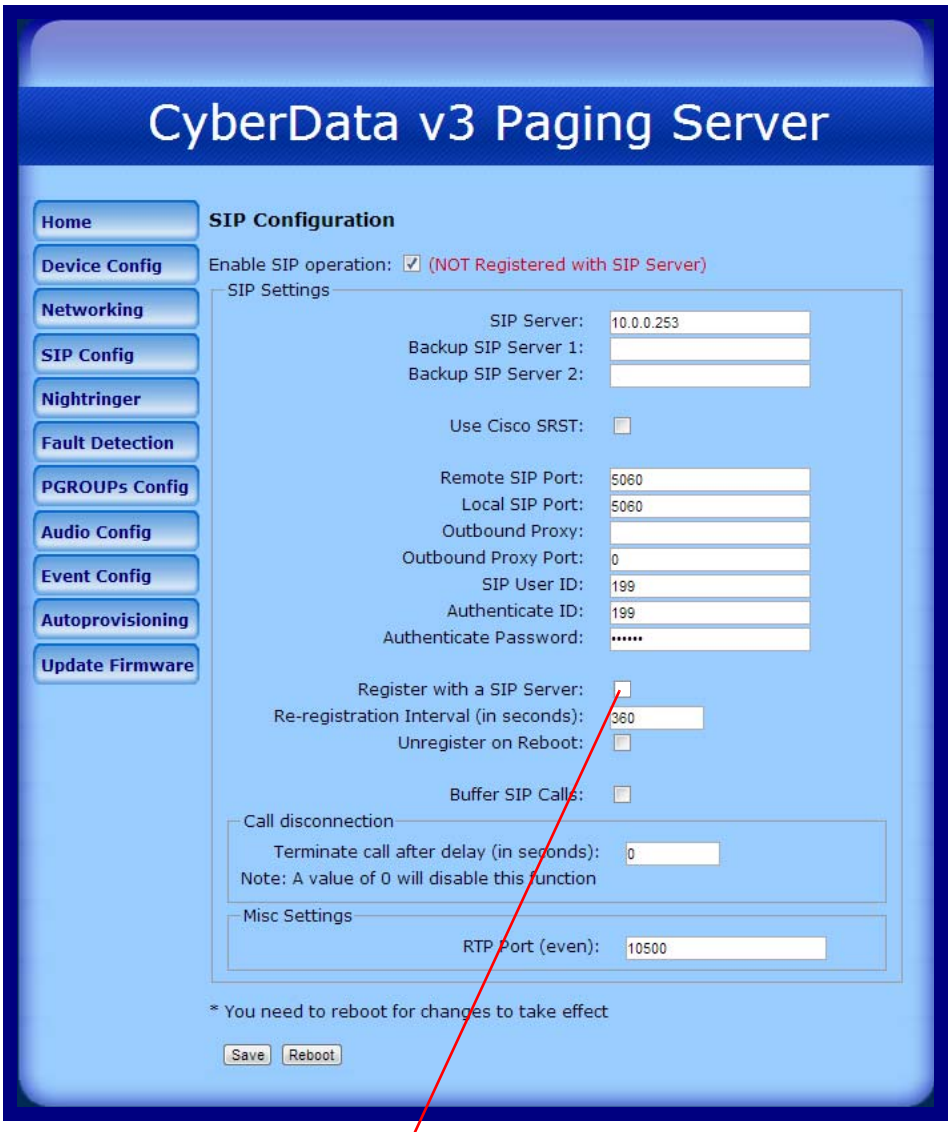
When the board is set to not register with a SIP server, it's possible to set the device to dial out to a single endpoint. To do this, do the following:

1. On the **SIP Configuration** page (Figure 2-13), make sure that the **Register with a SIP Server** parameter is not selected.
2. Type the IP address of the remote device that you want to contact into the **Dial out Extension** field

Note The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Establishing point-to-point SIP calls may not work with all phones.

Figure 2-13. SIP Configuration Page Set to Point-to-Point Mode



Device is set to **NOT** register with a SIP server

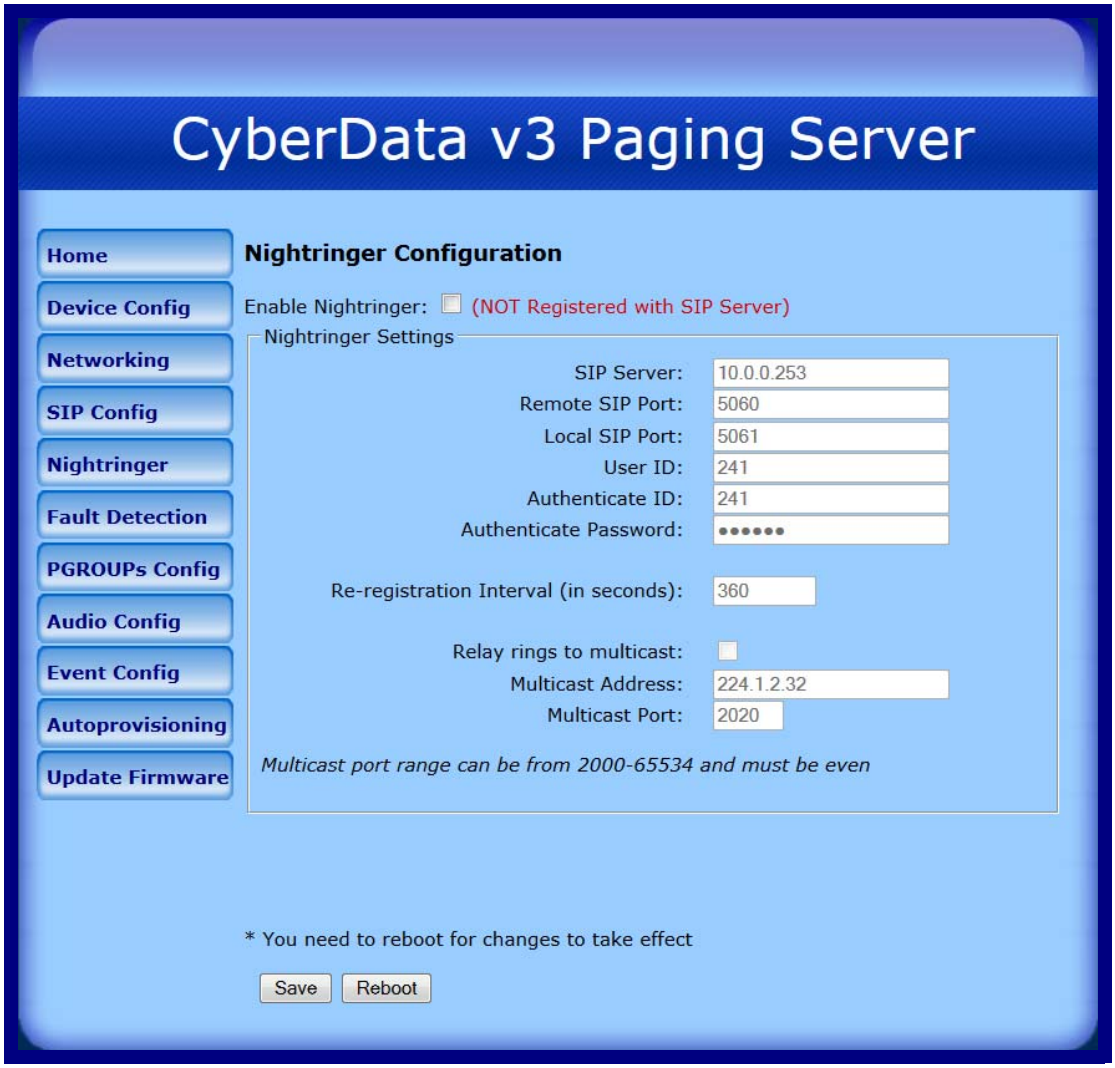
2.4.7 Configure the Night Ringer Parameters

Caution

Nightringer requires SIP Registration. Nightringer cannot be used in peer to peer mode.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See Figure 2-14.

Figure 2-14. Nightringer Configuration Page



2. On the **Nightringer Configuration** page, enter values for the parameters indicated in Table 2-9.

Table 2-9. Nightringer Configuration Parameters

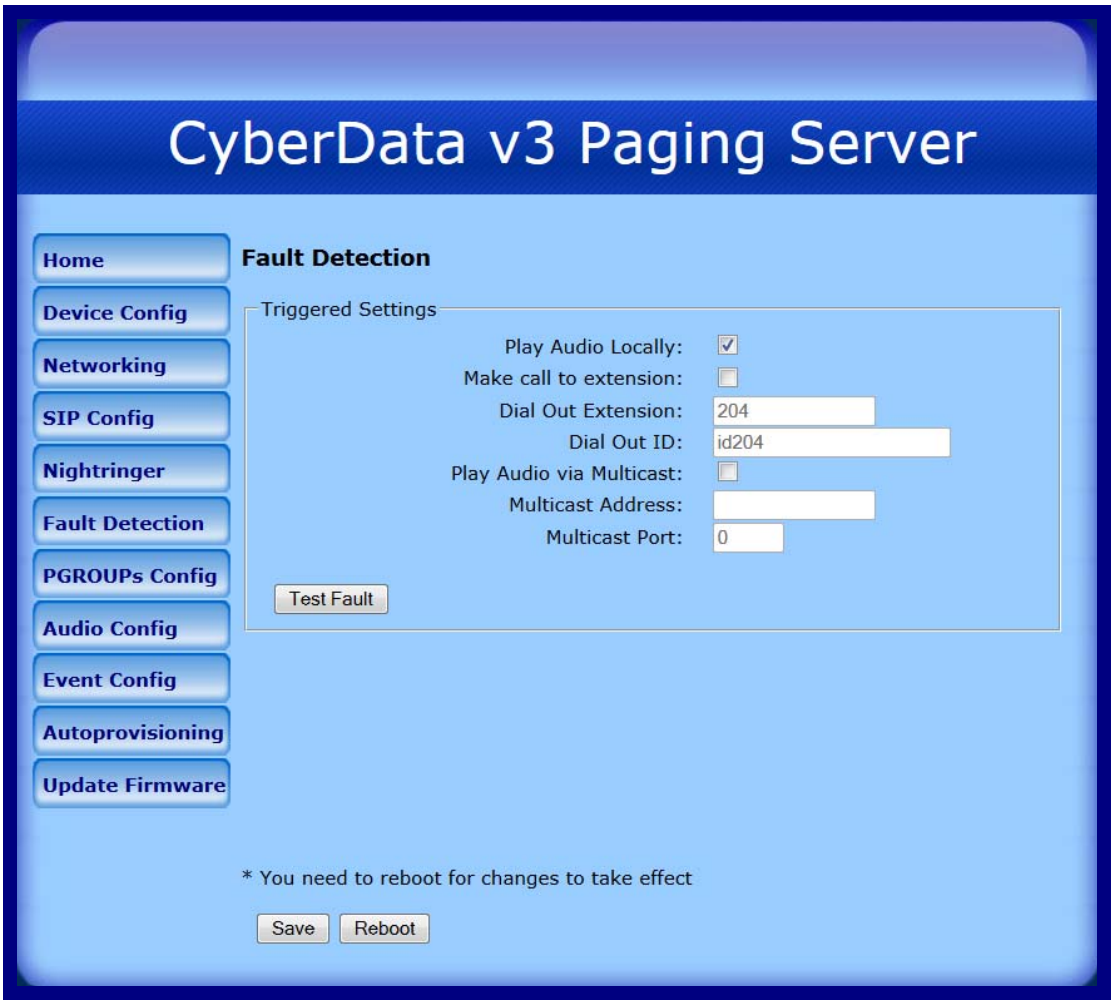
Web Page Item	Description
Enable Nightringer	When the nightringer is enabled, the unit will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone.
Nightringer Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (5 character limit [values from 1 to 65535]).
Local SIP Port	Type the Local SIP Port number (default 5061) (5 character limit [values from 2000 to 65535]). **Note**: This value cannot be the same as the **Local SIP Port** found on the **SIP Configuration Page**.
User ID	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)	Type the SIP Registration lease time in seconds (default is 60 minutes) (4 character limit [values from 30 to 3600]). Re-registration Interval (in seconds)
Relay Rings to Multicast	When selected, a user-defined audio file is sent to the specified multicast address and port when the night ringer is activated.
Multicast Address	Type the Multicast address.
Multicast Port	Type the Multicast port number.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.
4. Click **Reboot** for the new settings to take effect.

2.4.8 Configure the Fault Detection Parameters

1. Click on the **Fault Detection** button to open the **Fault Detection Configuration** page. See Figure 2-15.

Figure 2-15. Fault Detection Configuration Page



2. On the **Fault Detection Configuration** page, enter values for the parameters indicated in Table 2-10.

Table 2-10. Fault Detection Configuration Parameters

Web Page Item	Description
Triggered Settings	
Play Audio Locally	When selected, when the sensor is triggered, the audio file for "Sensor Triggered" will play out of the line-out and 600-Ohm connectors.
Make Call to Extension	When selected, when the sensor is triggered, the device will call the **Dial Out Extension** and play the "Sensor Triggered" audio file when someone answers.
Dial Out Extension	Enter the Dial Out Extension that you want the device to call when the sensor is triggered.
Dial Out ID	Enter the caller ID for **Dial Out Extension**.
Play Audio via Multicast	When selected, the device will play the "Sensor Triggered" audio file via multicast when the sensor is triggered.
Multicast Address	Enter the multicast IP address (15 character limit).
Multicast Port	Enter the multicast port number (5 character limit).
Test Fault	Click on the **Test Fault** button to test the fault detection feature.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.
4. Click **Reboot** for the new settings to take effect.

2.4.9 Configure the Paging Groups (PGROUPS) Parameters

Note A PGROUP is a way of assigning multicast addresses and port numbers when configuring multicast paging speakers.

To assign a multicast address, you must first configure the speakers that you want to put into a paging zone by entering a particular multicast address and port number combination in the web configuration for these speakers.

Note The PGROUPS Configuration page consists of four pages. Each page must be saved independently.

1. Click on the **PGROUPS Config** button to open the **PGROUPS Configuration** page. See Figure 2-16.

Figure 2-16. PGROUPS Configuration Page

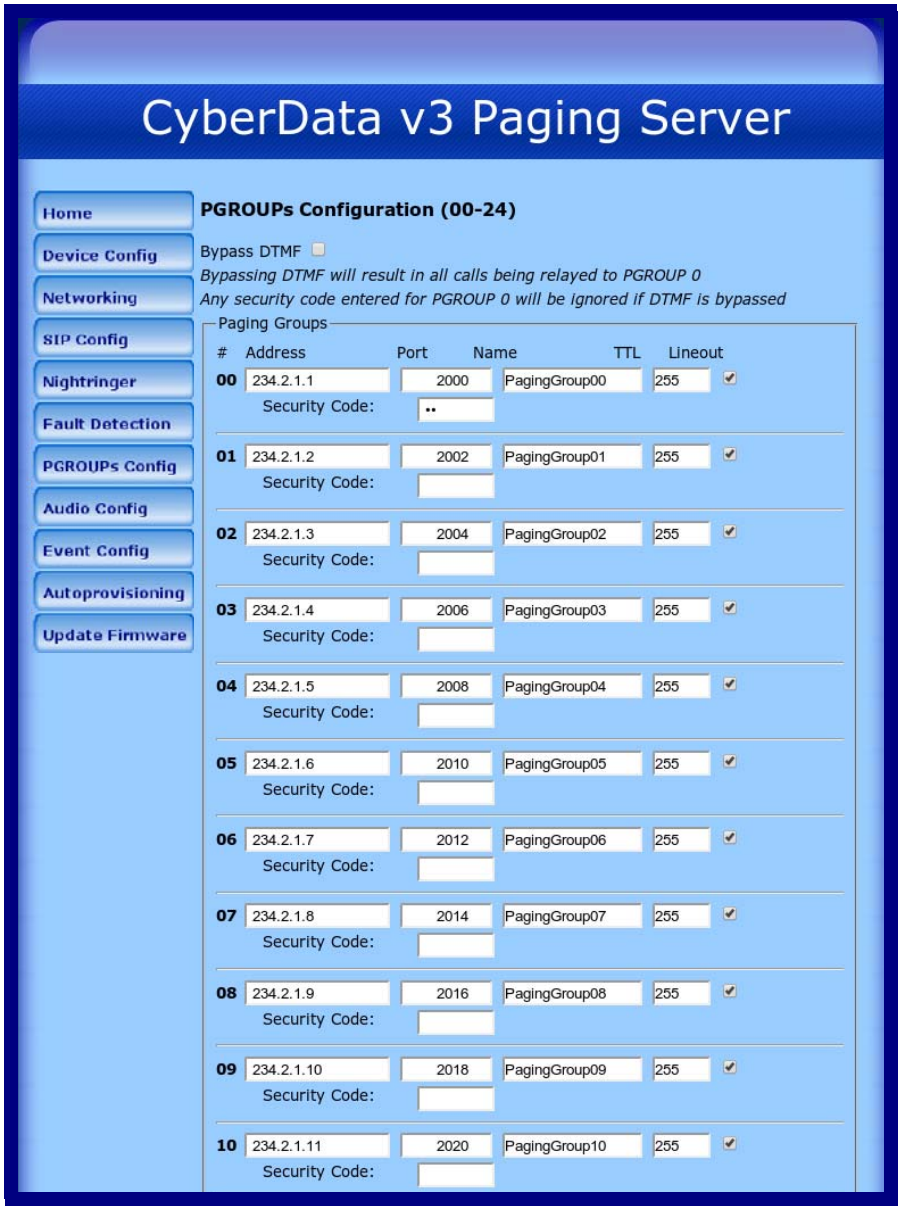


Figure 2-17. PGROUPS Configuration Page (continued)

Figure 2-18. PGROUPS Configuration Page (continued)

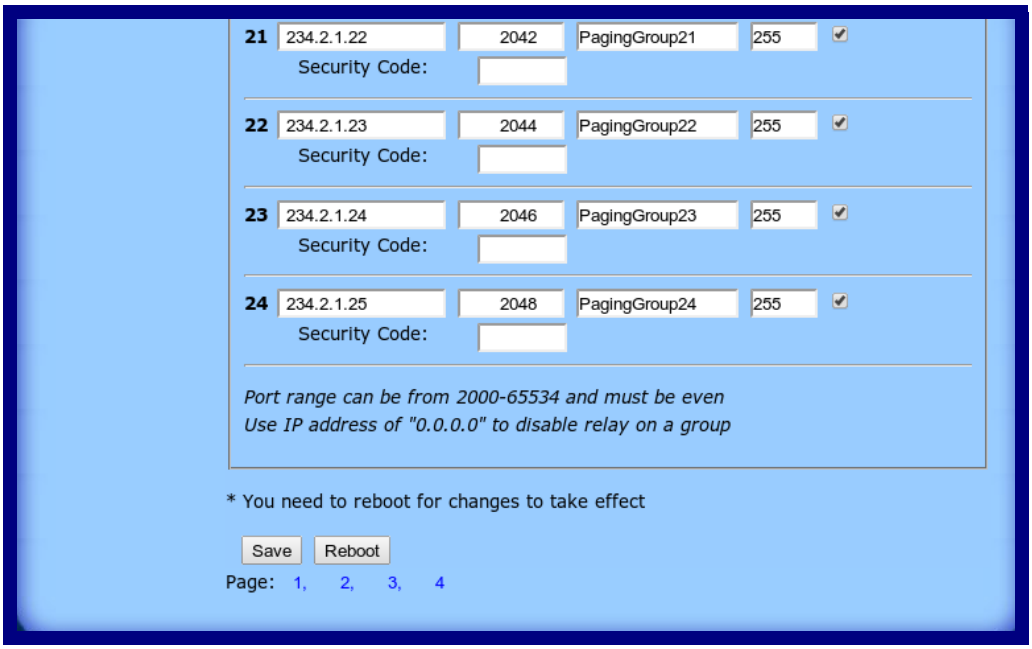

21 234.2.1.22 2042 PagingGroup21 255
Security Code:
22 234.2.1.23 2044 PagingGroup22 255
Security Code:
23 234.2.1.24 2046 PagingGroup23 255
Security Code:
24 234.2.1.25 2048 PagingGroup24 255
Security Code:
Port range can be from 2000-65534 and must be even
Use IP address of "0.0.0.0" to disable relay on a group
* You need to reboot for changes to take effect
Save
Reboot
Page: 1, 2, 3, 4

Figure 2-19. PGROUPS Configuration Page (continued)

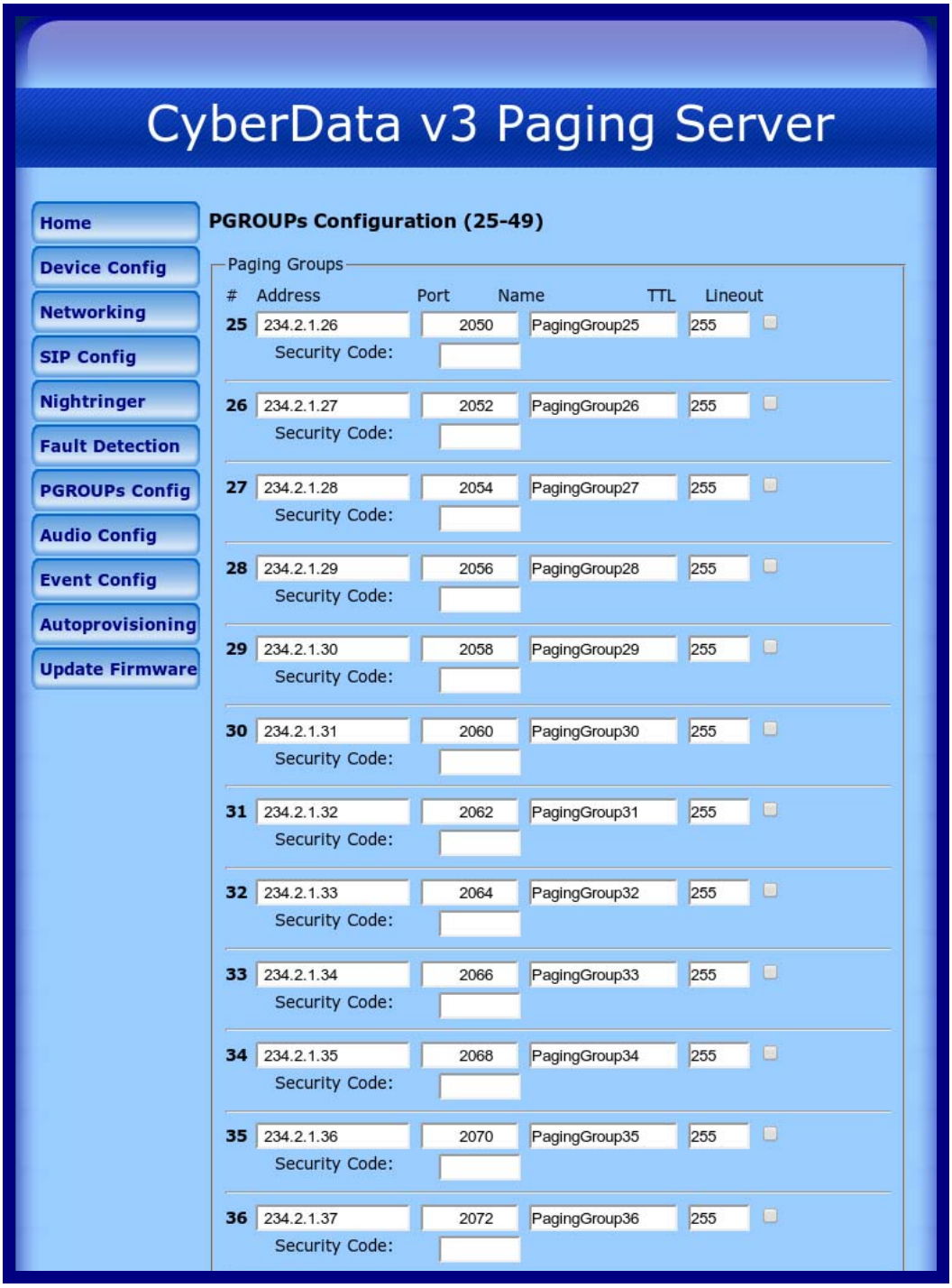


Figure 2-20. PGROUPS Configuration Page (continued)

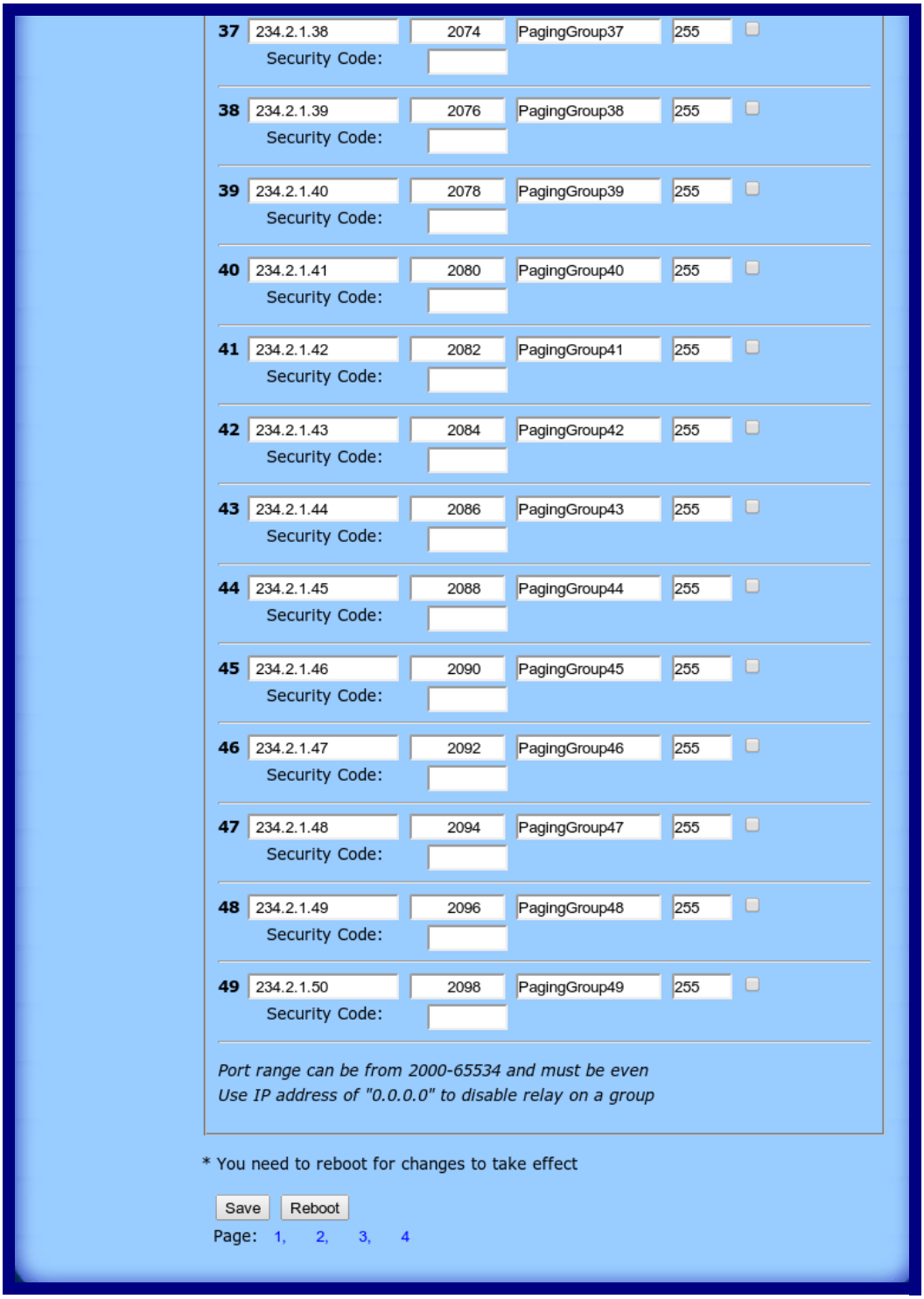

37 234.2.1.38 2074 PagingGroup37 255
Security Code:
38 234.2.1.39 2076 PagingGroup38 255
Security Code:
39 234.2.1.40 2078 PagingGroup39 255
Security Code:
40 234.2.1.41 2080 PagingGroup40 255
Security Code:
41 234.2.1.42 2082 PagingGroup41 255
Security Code:
42 234.2.1.43 2084 PagingGroup42 255
Security Code:
43 234.2.1.44 2086 PagingGroup43 255
Security Code:
44 234.2.1.45 2088 PagingGroup44 255
Security Code:
45 234.2.1.46 2090 PagingGroup45 255
Security Code:
46 234.2.1.47 2092 PagingGroup46 255
Security Code:
47 234.2.1.48 2094 PagingGroup47 255
Security Code:
48 234.2.1.49 2096 PagingGroup48 255
Security Code:
49 234.2.1.50 2098 PagingGroup49 255
Security Code:
Port range can be from 2000-65534 and must be even
Use IP address of "0.0.0.0" to disable relay on a group
* You need to reboot for changes to take effect
Save
Reboot
Page: 1, 2, 3, 4

Figure 2-21. PGROUPS Configuration Page (continued)

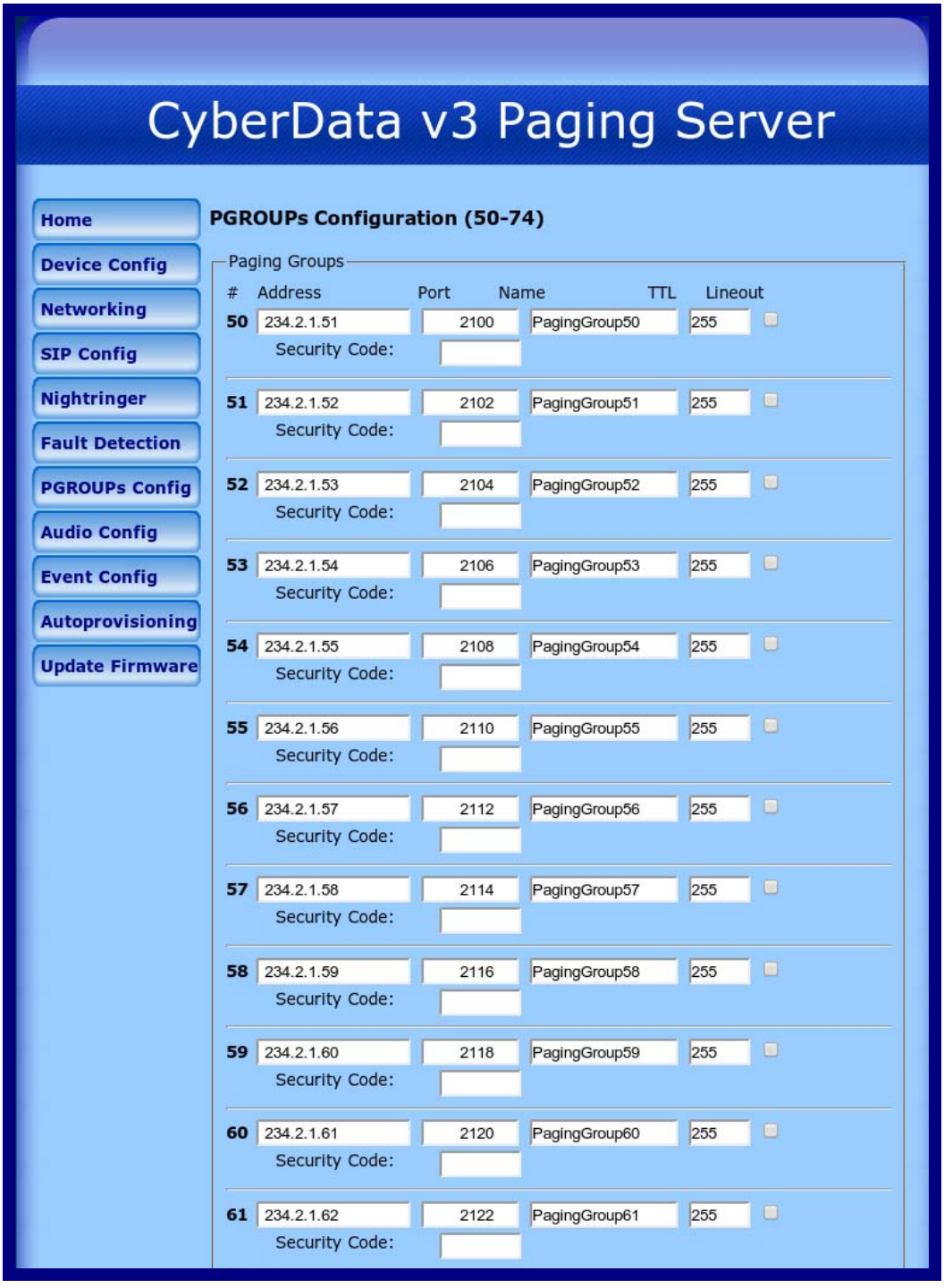


Figure 2-22. PGROUPS Configuration Page (continued)

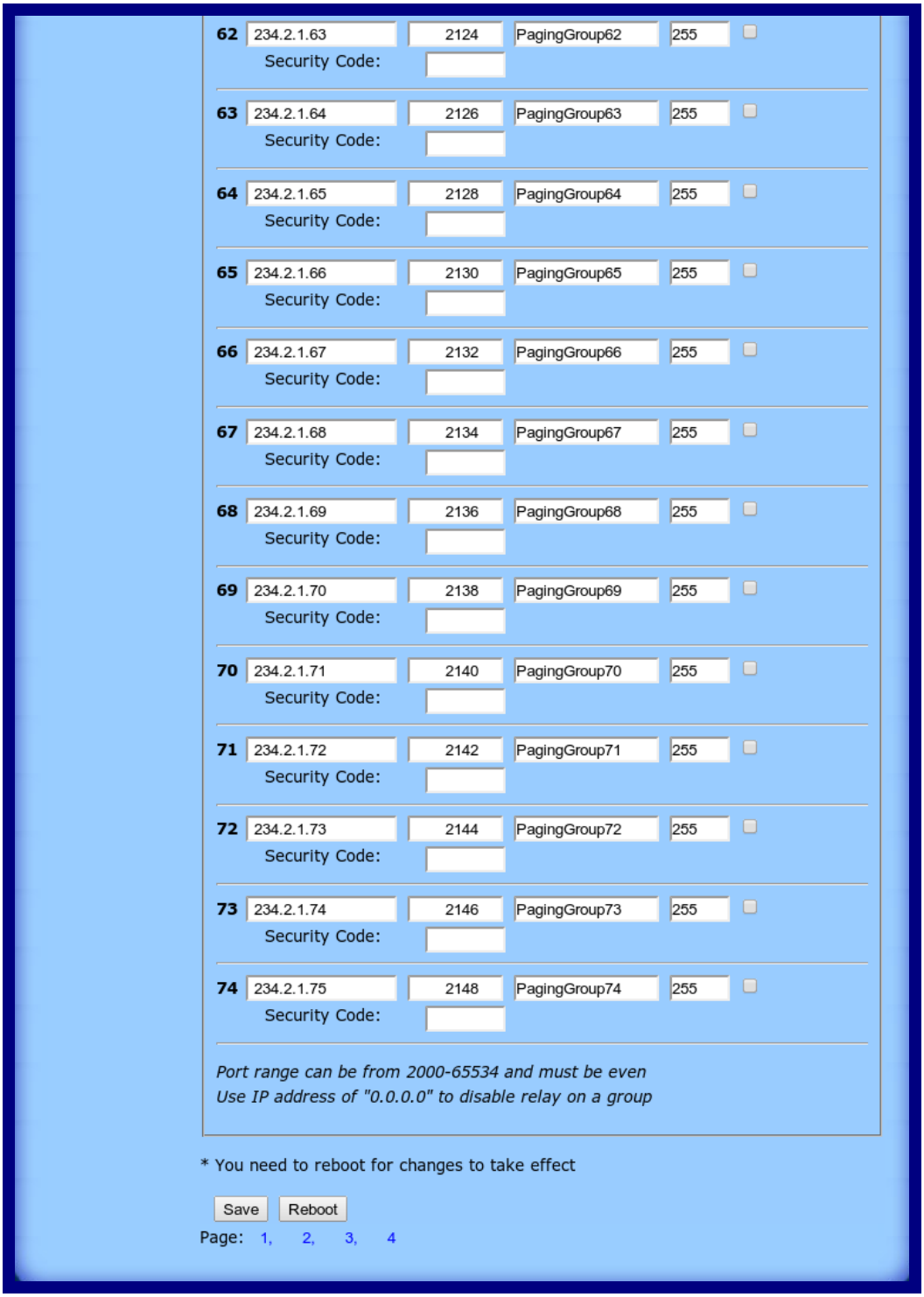

62 234.2.1.63 2124 PagingGroup62 255
Security Code:
63 234.2.1.64 2126 PagingGroup63 255
Security Code:
64 234.2.1.65 2128 PagingGroup64 255
Security Code:
65 234.2.1.66 2130 PagingGroup65 255
Security Code:
66 234.2.1.67 2132 PagingGroup66 255
Security Code:
67 234.2.1.68 2134 PagingGroup67 255
Security Code:
68 234.2.1.69 2136 PagingGroup68 255
Security Code:
69 234.2.1.70 2138 PagingGroup69 255
Security Code:
70 234.2.1.71 2140 PagingGroup70 255
Security Code:
71 234.2.1.72 2142 PagingGroup71 255
Security Code:
72 234.2.1.73 2144 PagingGroup72 255
Security Code:
73 234.2.1.74 2146 PagingGroup73 255
Security Code:
74 234.2.1.75 2148 PagingGroup74 255
Security Code:
Port range can be from 2000-65534 and must be even
Use IP address of "0.0.0.0" to disable relay on a group
* You need to reboot for changes to take effect
Save
Reboot
Page: 1, 2, 3, 4

Figure 2-23. PGROUPS Configuration Page (continued)

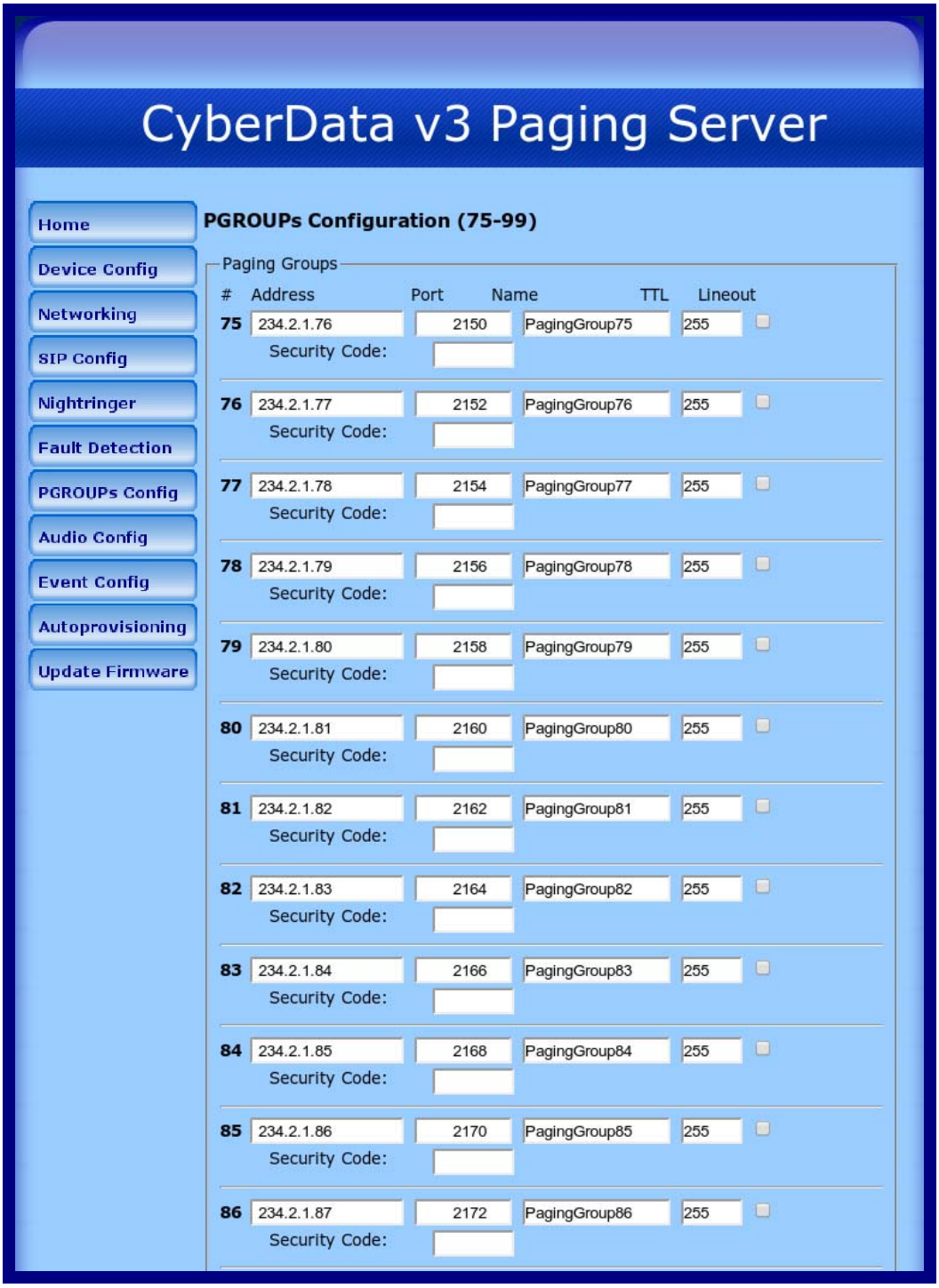
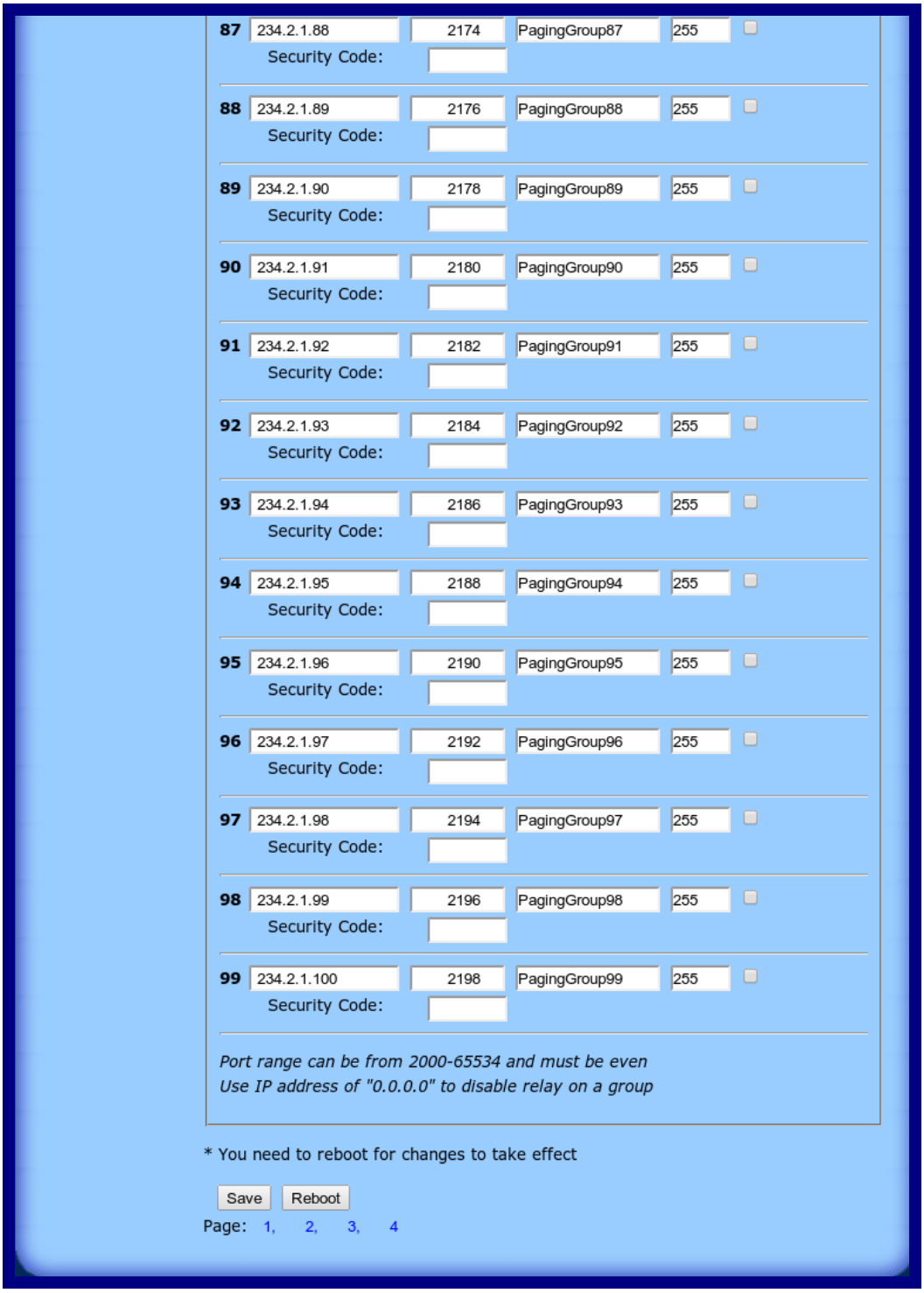


Figure 2-24. PGROUPS Configuration Page (continued)


87 234.2.1.88 2174 PagingGroup87 255
Security Code:
88 234.2.1.89 2176 PagingGroup88 255
Security Code:
89 234.2.1.90 2178 PagingGroup89 255
Security Code:
90 234.2.1.91 2180 PagingGroup90 255
Security Code:
91 234.2.1.92 2182 PagingGroup91 255
Security Code:
92 234.2.1.93 2184 PagingGroup92 255
Security Code:
93 234.2.1.94 2186 PagingGroup93 255
Security Code:
94 234.2.1.95 2188 PagingGroup94 255
Security Code:
95 234.2.1.96 2190 PagingGroup95 255
Security Code:
96 234.2.1.97 2192 PagingGroup96 255
Security Code:
97 234.2.1.98 2194 PagingGroup97 255
Security Code:
98 234.2.1.99 2196 PagingGroup98 255
Security Code:
99 234.2.1.100 2198 PagingGroup99 255
Security Code:
Port range can be from 2000-65534 and must be even
Use IP address of "0.0.0.0" to disable relay on a group
* You need to reboot for changes to take effect
Save
Reboot
Page: 1, 2, 3, 4

2. On the **PGROUPS Configuration** page, enter values for the parameters indicated in Table 2-11.

Table 2-11. PGROUPS Configuration Parameters

Web Page Item	Description
Bypass DTMF	When selected, bypassing the DTMF will result in all calls being relayed to PGROUP 0.
#	Shows the paging group number.
Address	Enter the IP address of the PGROUP. **Note**: To disable a relay on a group, use an IP address of *0.0.0.0*.
Port	Enter the port number of the PGROUP. **Note**: The port range can be from 2000 to 65534 and must be even.
Name	Enter a name for the PGROUP.
TTL	The TTL field allows you to adjust the TTL. TTL is "time to live" and it describes how many networks (routers) a packet will go through before it is discarded.
Lineout	The Lineout field determines whether or not the device will play audio out of the RCA output port and the 600 Ohm output port in addition to forwarding it to the PGROUP.
Security Code	This field allows the user to add a security code to prevent unauthorized paging to the PGROUP. Code must be between two to five numeric digits (**0** through **9**). Leave the field empty for no security code. Any security code entered for PGROUP **0** will be ignored if DTMF is bypassed.
Page: 1 2 3 4	Click on **1**, **2**, **3**, or **4** to navigate through the pages of PGROUPS.

3. After changing the parameters, click **Save Settings**.

2.4.10 Operating the Paging Server

Call behavior changes based on the configuration of the **PGROUPs Configuration** page.

2.4.10.1 DTMF Bypassed

- When the V3 Paging Server is called, it will send the "page tone" audio message to the caller.
- When the caller hears this message, the caller should begin speaking.

2.4.10.2 DTMF Not Bypassed

- When the V3 Paging Server is called, it sends the "Enter PGROUP" audio message to the caller. By default, this message is "Enter the two digit zone number."
- When the caller hears this message, the caller should enter the two-digit code for the zone that the caller wants to page.
- If the zone is invalid or not configured, the V3 Paging Server sends the "Invalid PGROUP" audio message to the caller. By default this message is "Invalid zone number. Enter the two digit zone number." The caller should repeat the previous step.
- If a security code is enabled on the zone, the V3 Paging Server sends the "Enter Code" audio message to the caller. By default this message is "Enter the security code." When the caller hears this message, the caller should enter the security code for the selected zone. If no security code is enabled on the zone, the V3 Paging Server will send the "page tone" audio message to the caller. The caller should begin speaking when this message is heard.
- If the security code is invalid, the V3 Paging Server will send the "Invalid Code" audio message to the caller. By default this message is "Invalid Security code. Enter the security code." The caller should repeat the previous step. When a valid security code is entered, the V3 Paging Server will send the "page tone" audio message to the caller. The caller should begin speaking when this message is heard.
- For *page-all*, you simply configure *all* speakers with a particular multicast address and port number combination, which represents one of the 100 zones that the paging server will initially support. Each speaker can still be part of 100 other paging zones in addition to the one *page-all* zone.
- The V3 Paging Server can negotiate the multicast stream via SIP regardless of the bypass state. However, if the V3 Paging Server is not in bypass mode (or the multicast sender does not send any DTMF), the device will not play or relay any audio because the device will be waiting at the zone entry prompt. The DTMF from the sender would have to be sent as RFC2833 RTP events (i.e. "out of band").

2.4.11 Configure the Audio Parameters

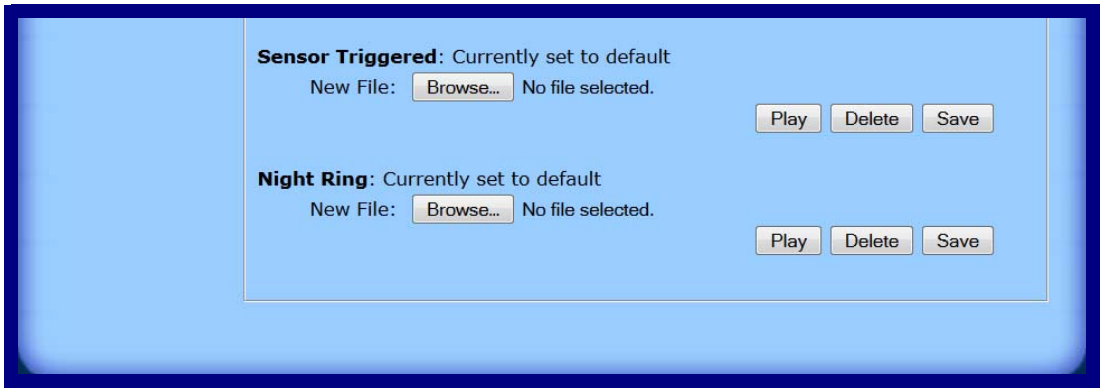
Click on the **Audio Config** button to open the **Audio Configuration** page. See Figure 2-25. The **Audio Configuration** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

Figure 2-25. Audio Configuration Page

Figure 2-26. Audio Configuration Page

9: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Dot: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Audio test: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Page tone: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Enter PGROUP: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Invalid PGROUP: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Enter Code: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Invalid Code: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Your IP Address is: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Rebooting: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Restoring Default: Currently set to default
New File: Browse... No file selected.
Play Delete Save

Figure 2-27. Audio Configuration Page


Sensor Triggered: Currently set to default
New File: Browse... No file selected.
Play Delete Save
Night Ring: Currently set to default
New File: Browse... No file selected.
Play Delete Save

On the **Audio Configuration** page, enter values for the parameters indicated in Table 2-12.

Note Each entry on the **Audio Configuration** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the V3 Paging Server is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

Table 2-12. Audio Configuration Parameters

Web Page Item	Description
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit).
Audiotest	Corresponds to the message “This is the CyberData IP speaker test message...” (24 character limit).
Page tone	Corresponds to a simple tone that is unused by default (24 character limit).
Enter PGROUP	Corresponds to the message “Enter PGROUP” (24 character limit).
Invalid PGROUP	Corresponds to the message “Invalid PGROUP” (24 character limit).
Enter Code	Corresponds to the message “Enter Code” (24 character limit).
Invalid Code	Corresponds to the message “Invalid Code” (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring default	Corresponds to the message “Restoring default” (24 character limit).
Sensor Triggered	Corresponds to the message “Sensor Triggered” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
	The **Browse** button will allow you to navigate to and select an audio file.
	The **Play** button will play that audio file.
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.

Table 2-12. Audio Configuration Parameters (continued)

Web Page Item	Description
Save	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.4.11.1 User-created Audio Files

User-created audio files must be saved in one of the following formats:

- RIFF (little-endian) data,
- WAVE audio, Microsoft PCM
- 16 bit, mono 8000 Hz

Note These audio format restrictions are enforced by the webpage.

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-28 through Figure 2-30.

Figure 2-28. Audacity 1

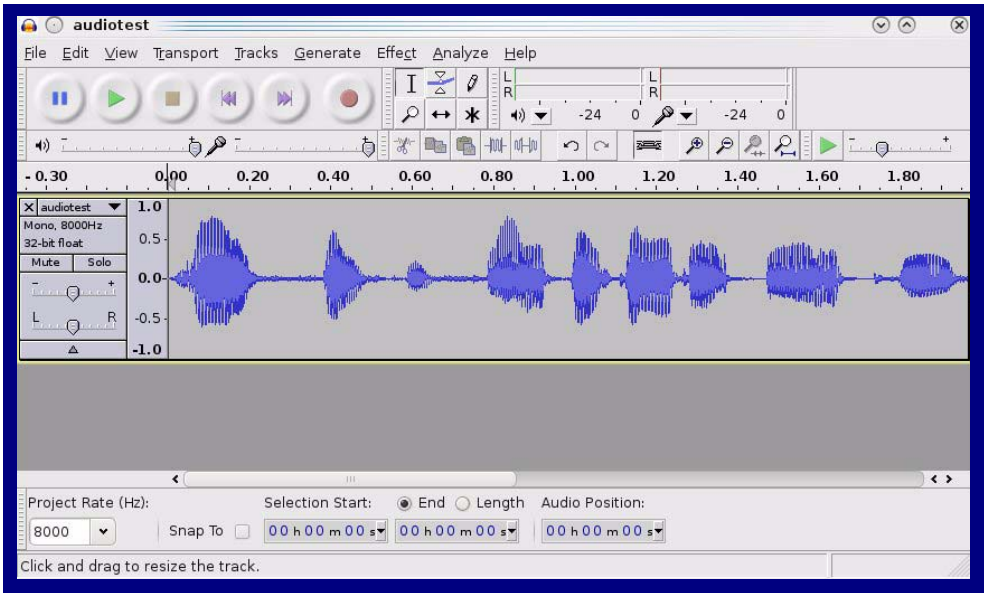
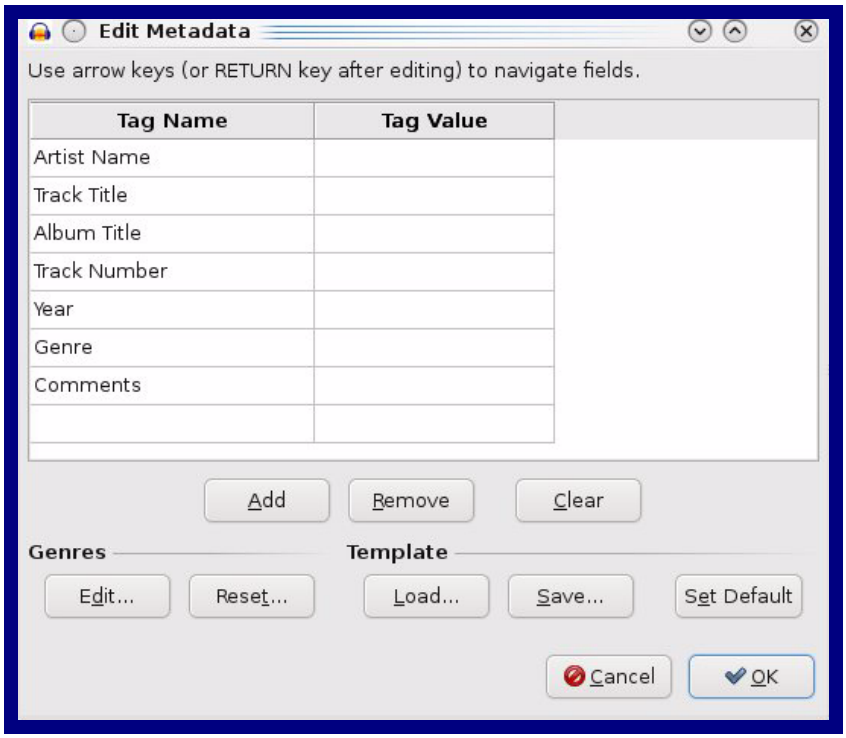


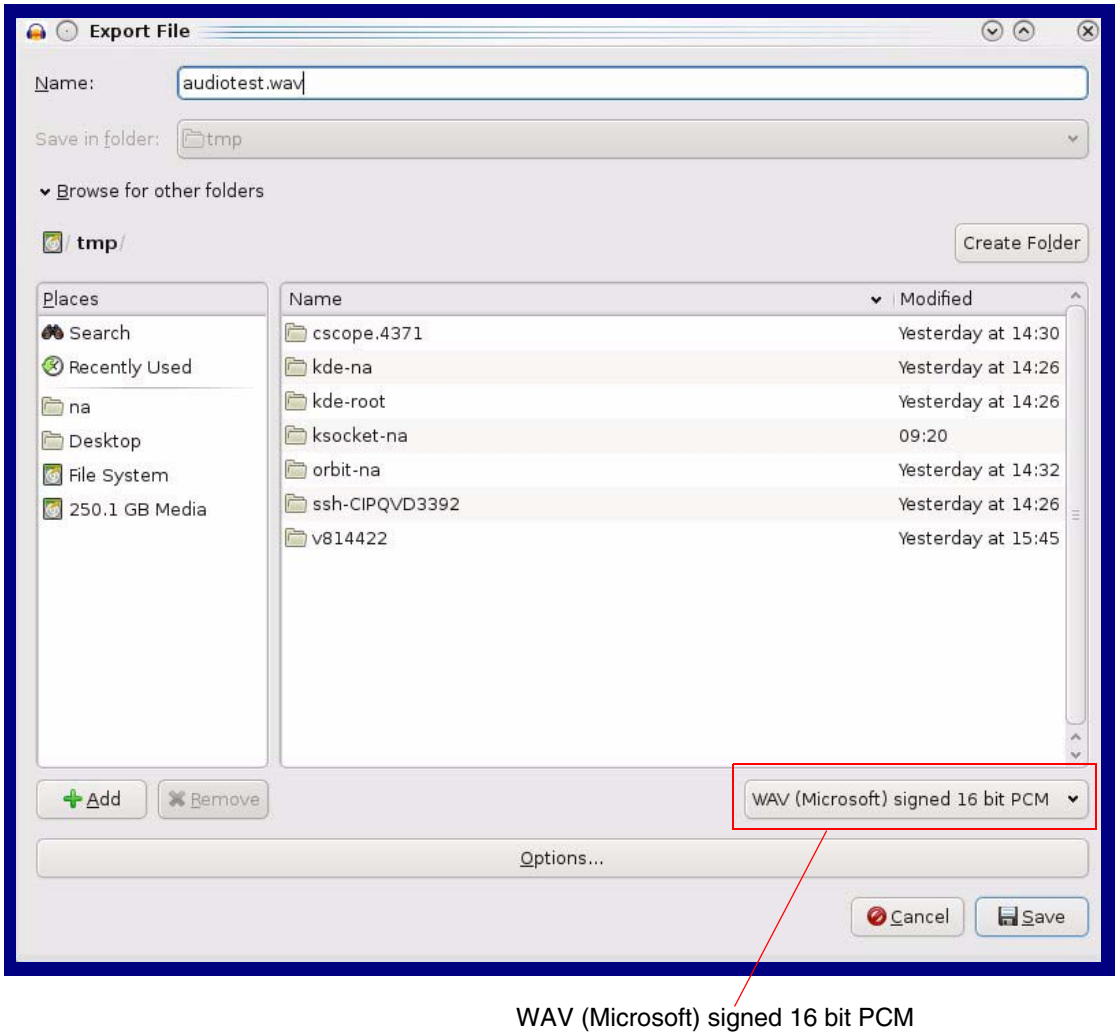
Figure 2-29. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-30. WAV (Microsoft) signed 16 bit PCM



2.4.12 Configure the Event Parameters

Click on the **Event Config** button to open the **Event Configuration** page (Figure 2-31). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-31. Event Configuration Page

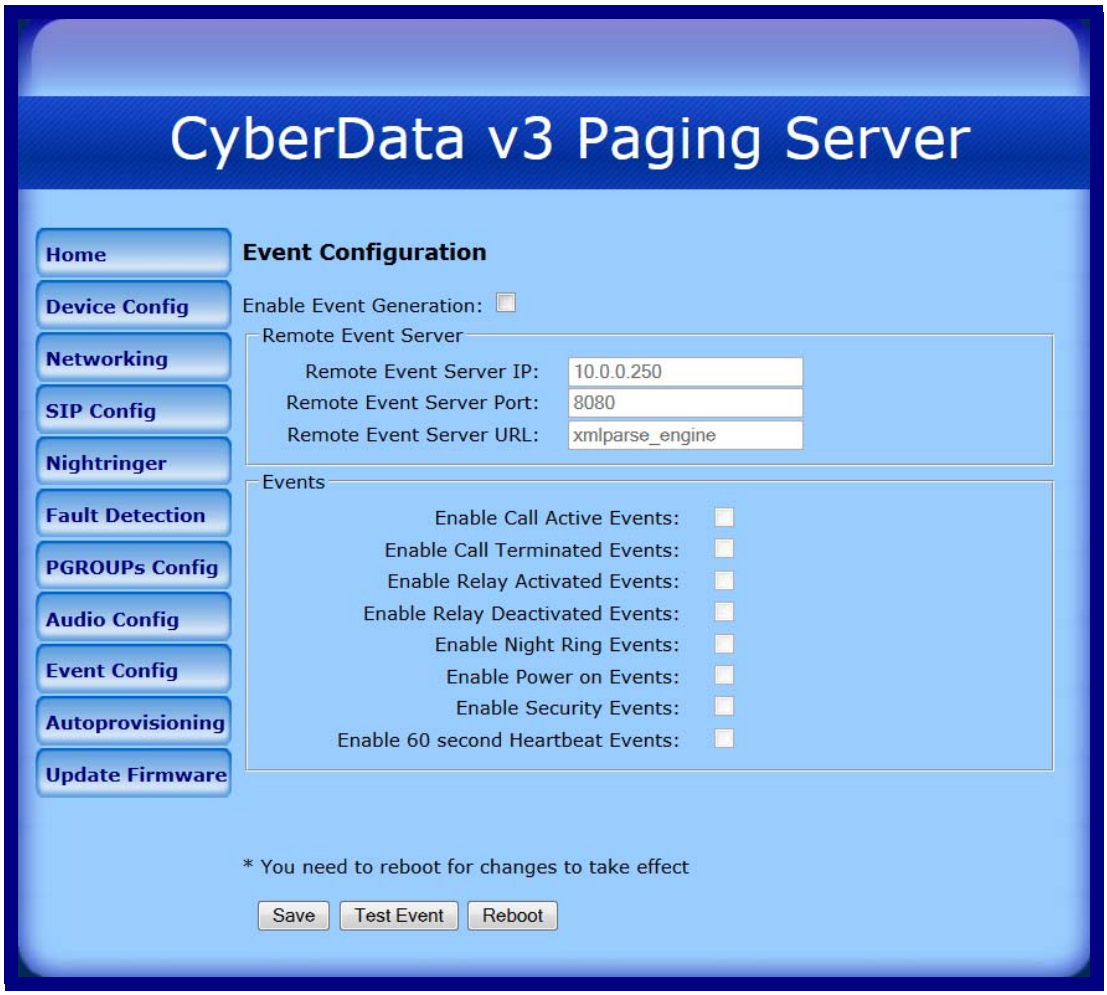


Table 2-13 shows the web page items on the **Event Configuration** page.

Table 2-13. Event Configuration

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
Remote Event Server	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
Events	
Enable Call Active Events	When selected, Call Active Events are enabled.
Enable Call Terminated Events	When selected, Call Terminated Events are enabled.
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the unit receives a night ring.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Security Events	When selected, Security Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Event	Click on the **Test Event** button to test an event.
Reboot	Click on the **Reboot** button to reboot the system.

2.4.12.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

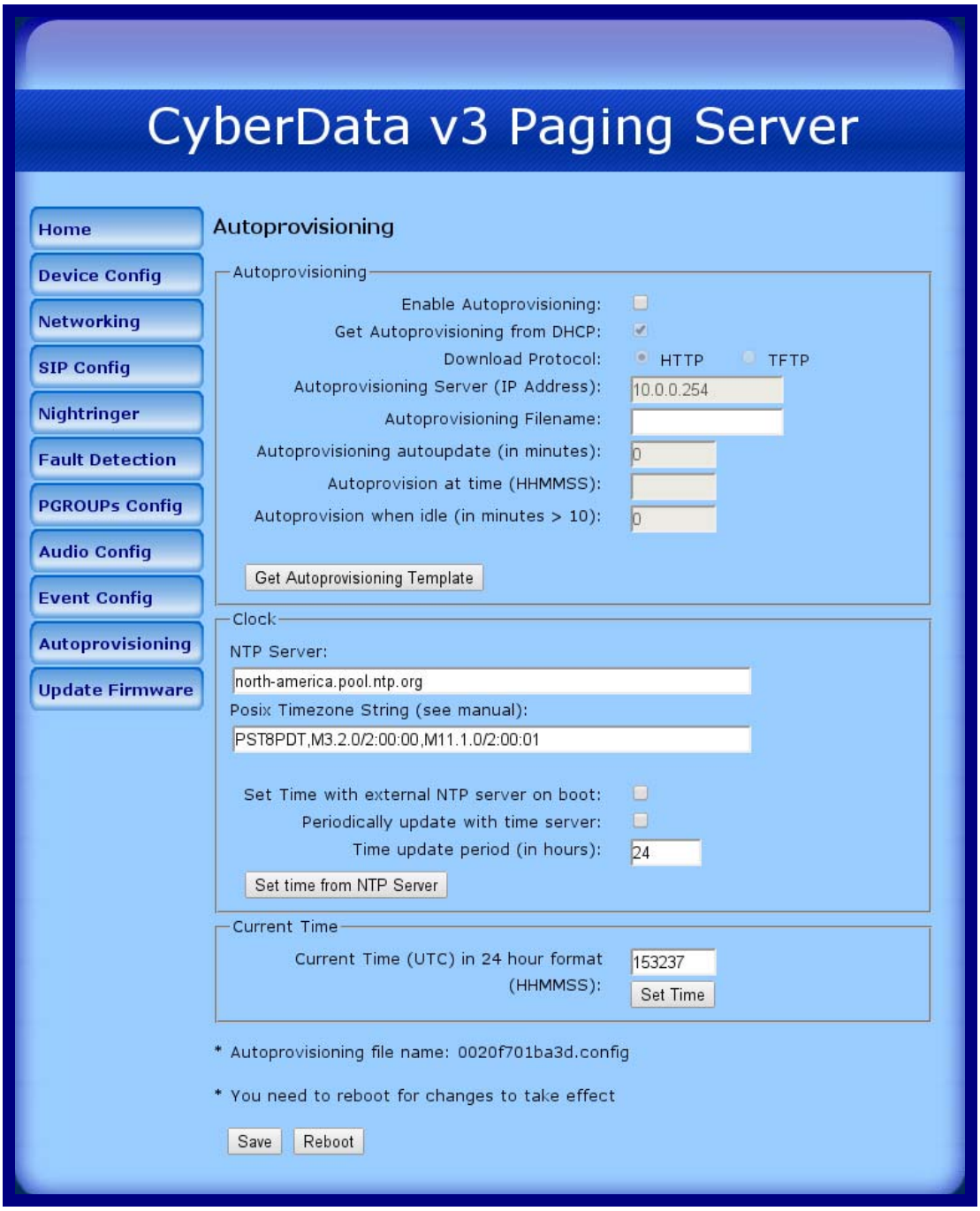
```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.4.13 Configure the Autoprovisioning Parameters

1. Click on the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See Figure 2-32.

Figure 2-32. Autoprovisioning Configuration Page



2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 2-14.

Table 2-14. Autoprovisioning Configuration Parameters

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning	See Section 2.4.13.1, "Autoprovisioning".
Get Autoprovisioning from DHCP	See Section 2.4.13.1, "Autoprovisioning".
Download Protocol	Allows you to select whether the autoprovisioning file is acquired via **TFTP** or **HTTP**.
Autoprovisioning Server (IP Address)	See Section 2.4.13.1, "Autoprovisioning" (15 character limit).
Autoprovisioning Filename	Type the desired name for the autoprovisioning file.
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
Autoprovision at time (HHMMSS)	Type the desired time of day that you want the Autoprovisioning feature to update (must be 6 characters).
Autoprovision when idle (in minutes > 10)	Type the desired time (in minutes greater than 10) that you want the Autoprovisioning feature to update after a certain amount of idle time (6 character limit).
Get Autoprovisioning Template	Press the **Get Autoprovisioning Template** button to create an autoprovisioning file for this unit. See Section 2.4.13.2, "Get Autoprovisioning Template Button"
Clock	
NTP Server	Allows you to select the NTP server (64 character limit).
Posix Timezone String	See Section 2.4.13.3, "Time Zone Strings" (43 character limit).
Set Time with External NTP Server on boot	When selected, the time is set with an external NTP server when the device restarts.
Periodically update with time server	When selected, the time is periodically updated with a time server.
Time update period (in hours)	Allows you to select the time updated period (in hours) (4 character limit).
Set time from NTP Server	Allows you to set the time from the NTP server.
Current Time	
Current Time (UTC) in 24 hour format (**HHMMSS**)	Allows you to input the current time in the 24 hour format. (6 character limit)
Set Time	Click on this button to set the clock after entering the current time.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.4.13.1 Autoprovisioning

Enable Autoprovisioning Option

With autoprovisioning enabled, the board will get its configuration from a remote TFTP or HTTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP or HTTP server. The user generates or downloads a template for this XML file through the web interface and the user can then modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP or HTTP server directory and manually set the TFTP or HTTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <MiscSettings>
        <DeviceName>auto V3 Paging Server</DeviceName>
    </MiscSettings>

</specific>
```

Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
        max-lease-time 120;
        default-lease-time 120;

        option routers                  10.0.0.1;
        option subnet-mask              255.0.0.0;

        option domain-name              "voiplab";
        option domain-name-servers       10.0.0.1;

        option time-offset              -8;     # Pacific Standard Time

        option tftp-server-name         "10.0.0.254";

        option option-150               10.0.0.254;

        range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address)

Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate

If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades

An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v5.0.5b01</FirmwareVersion>
<FirmwareFile>505b01-uImage-ceilingspeak</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

Note For information about TFTP servers, see Appendix A: "Setting Up a TFTP Server".

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by one of the following two ways:

- Click **Delete** for each file that you want to restore to the factory default audio file on the **Audio Configuration** page**.**
- Change the autoprovisioning file with the word "***default***" set as the file name.

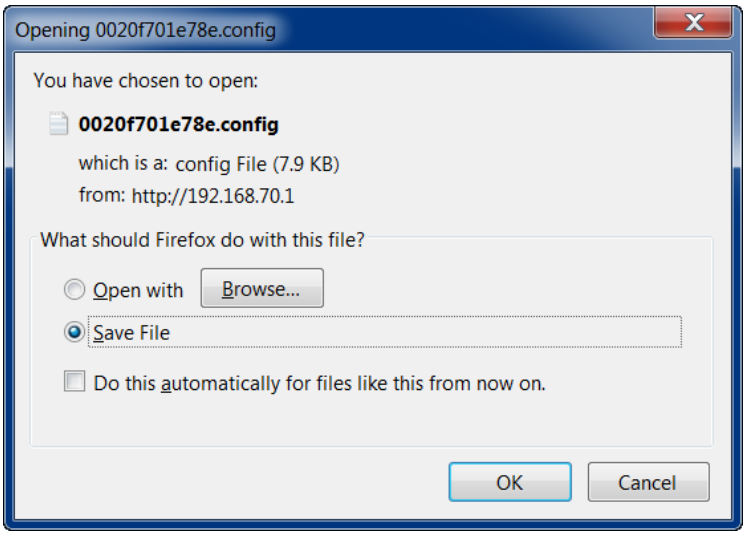
2.4.13.2 Get Autoprovisioning Template Button

The **Get Autoprovisioning Template** button allows the user to generate, download, edit, and then store an autoprovisioning template on the server that serves the autoprovisioning files for devices.

To generate an autoprovisioning template directly from the device, complete the following steps:

1. On the **Autoprovisioning** page, click on the **Get Autoprovisioning Template** button.
2. You will see a window prompting you to save a configuration file (**.config**) to a location on your computer (Figure 2-33). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See Figure 2-33.

Figure 2-33. Configuration File



4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.
5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.4.13.3 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Table 2-15 shows some common strings.

Table 2-15. Common Time Zone Strings

Time Zone	Time Zone String
US Pacific time	PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Mountain time	MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Eastern Time	EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
Phoenix Arizona[a]	MST7
US Central Time	CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00

a.Phoenix, Arizona does not use daylight savings time.

Table 2-16 shows a breakdown of the parts that constitute the following time zone string:

- ***CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00***

Table 2-16. Time Zone String Parts

Time Zone String Part	Meaning
CST6CDT	The time zone offset from GMT and three character identifiers for the time zone.
CST	Central Standard Time
6	The (hour) offset from GMT/UTC
CDT	Central Daylight Time
M3.2.0/2:00:00	The date and time when daylight savings begins.
M3	The third month (March)
.2	The 2nd occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change
M11.1.0/2:00:00	The date and time when daylight savings ends.
M11	The eleventh month (November)
.1	The 1st occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change

Time Zone String Examples

Table 2-17 has some more examples of time zone strings.

Table 2-17. Time Zone String Examples

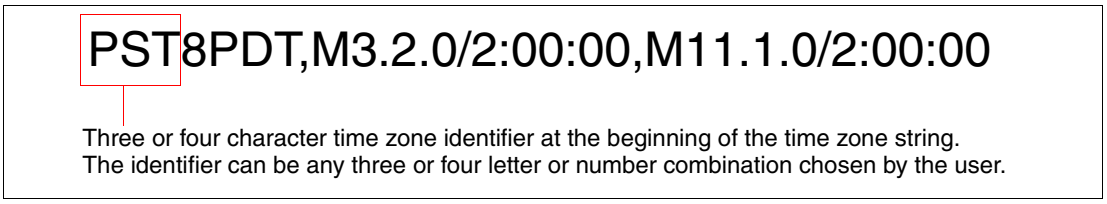
Time Zone	Time Zone String
Tokyo[a]	IST-9
Berlin[b]	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a.Tokyo does not use daylight savings time.
b.For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

Time Zone Identifier

A user-definable three or four character time zone identifier (such as PST, EDT, IST, MUT, etc) is needed at the beginning of the posix time zone string to properly set the time. However, the specific letters or numbers used for the time zone identifier are not important and can be any three or four letter or number combination that is chosen by the user. However, the time zone identifier cannot be blank.

Figure 2-34. Three or Four Character Time Zone Identifier


PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
Three or four character time zone identifier at the beginning of the time zone string.
The identifier can be any three or four letter or number combination chosen by the user.

You can also use the following URL when a certain time zone applies daylight savings time:

http://www.timeanddate.com/time/dst/2011.html

World GMT Table

Table 2-18 has information about the GMT time in various time zones.

Table 2-18. World GMT Table

Time Zone	City or Area Zone Crosses
GMT-12	Eniwetok
GMT-11	Samoa
GMT-10	Hawaii
GMT-9	Alaska
GMT-8	PST, Pacific US
GMT-7	MST, Mountain US
GMT-6	CST, Central US
GMT-5	EST, Eastern US
GMT-4	Atlantic, Canada
GMT-3	Brazilia, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time, Dublin

Table 2-18. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.5 Upgrading the Firmware

Note A new firmware signature prevents users from loading firmware intended for one device to a different device. See Table 2-19.

Table 2-19. Firmware

Firmware File Name	Description
700-uImage-pserver_nosig	Must be used to upgrade from previous versions to v7.0.0.
700-uImage-pserver_sig	Must be used to downgrade from versions greater than v7.0.0.
631-uImage-pserver_sig	Must be used to downgrade from v7.0.0 only to v6.3.1.

Caution

Equipment Hazard: Users will not be able to upgrade directly from versions older than v7.0.0 to versions greater than v7.0.0. Users will have to upgrade to v7.0.0 then move on from there.

2.5.1 Uploading the Firmware

1. Click on the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-35.

Figure 2-35. Upgrade Firmware Page

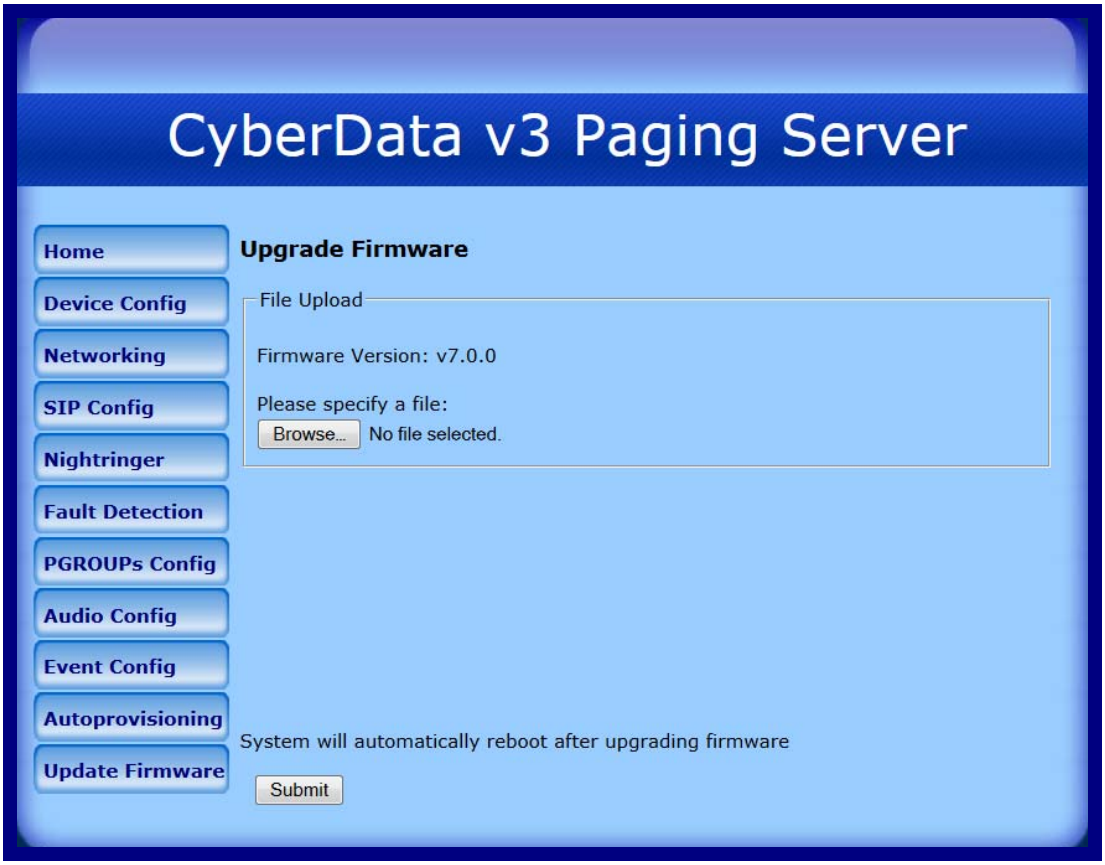


Table 2-20 shows the web page items on the **Upgrade Firmware** page.

Table 2-20. Upgrade Firmware Parameters

Web Page Item	Description
File Upload	
Firmware Version	Shows the current firmware version.
Please specify a file	Click on the **Browse** button to navigate to the application firmware file that you want to upload.
Browse...	The **Browse** button will allow you to navigate to and select an application firmware file.
Submit	Click on the **Submit** button to automatically upload the selected firmware and reboot the system.

2.5.1.1 Upgrade the Firmware

To upload the firmware from your computer:

1. Retrieve the latest V3 Paging Server firmware from the VoIP V3 Paging Server **Downloads** page at:

   http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/downloads.html

2. Unzip the V3 Paging Server version file. This file may contain the following:
   - Firmware file
   - Release notes
3. Log in to the V3 Paging Server home page as instructed in Section 2.4.3, "Log in to the Configuration GUI".
4. Click on the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-35.
5. Click **Browse**, and then navigate to the location of the V3 Paging Server firmware file.
6. Click **Submit**.

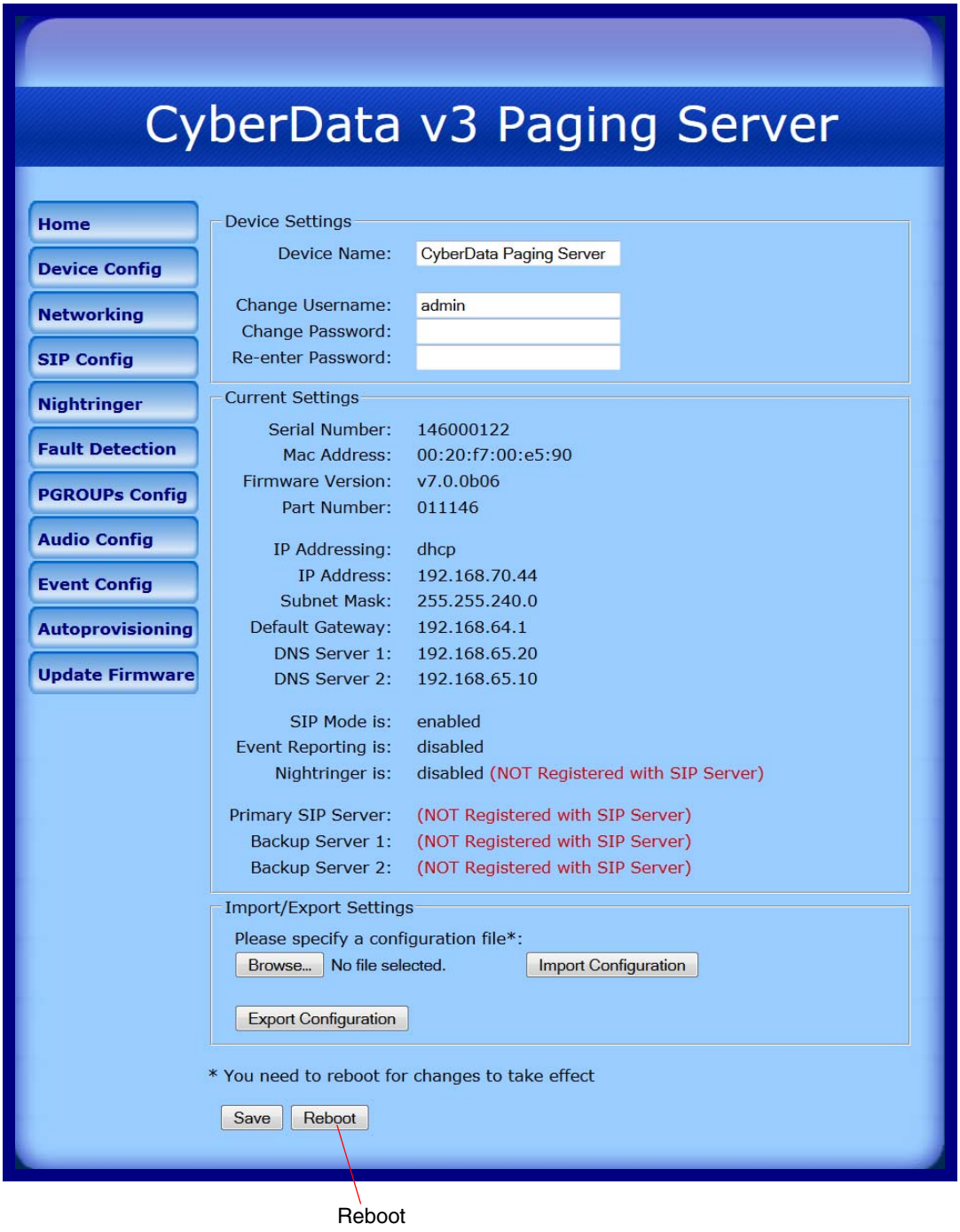
Note This starts the upload process. Once the V3 Paging Server has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The V3 Paging Server will automatically reboot when the upload is complete. When the countdown finishes, the **Upgrade Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

2.5.2 Reboot the V3 Paging Server

To reboot a V3 Paging Server, log in to the web page as instructed in Section 2.4.3, "Log in to the Configuration GUI".

1. Click **Reboot** (Figure 2-36). A normal restart will occur.

Figure 2-36. Home Page



2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-21 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.6.1 Command Interface Post Commands

These commands require an authenticated session (a valid username and password to work).

Table 2-21. Command Interface Post Commands[a]

Device Action	HTTP Post Command[1]
Trigger relay (fixed at 5 seconds)	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "test_relay=yes"
Terminate active call	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "reboot=yes"
Play “audio test message”	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_3=yes"
Play the "4" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_6=yes"

Table 2-21. Command Interface Post Commands[a] (continued)

Play the "7" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_d=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_restoringdefault=yes"
Play the "Sensor Triggered" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_sensortriggered=yes"
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_nightring=yes"
Play the "Enter PGROUP" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_enterpgroup=yes"
Play the "Invalid PGROUP" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_invalidpgroup=yes"
Play the "Enter Code" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_entercode=yes"
Play the "Invalid Code" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_invalidcode=yes"

Table 2-21. Command Interface Post Commands[a] (continued)

Delete the "0" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_0=yes"
Delete the "1" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_1=yes"
Delete the "2" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_2=yes"
Delete the "3" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_3=yes"
Delete the "4" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_4=yes"
Delete the "5" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_5=yes"
Delete the "6" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_6=yes"
Delete the "7" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_7=yes"
Delete the "8" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_8=yes"
Delete the "9" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_9=yes"
Delete the "Audio Test" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_audiotest=yes"
Delete the "Page Tone" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_pagetone=yes"
Delete the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_youripaddressis=yes"
Delete the "Rebooting" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_rebooting=yes"
Delete the "Restoring Default" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_restoringdefault=yes"

Table 2-21. Command Interface Post Commands[a] (continued)

Delete the "Sensor Triggered" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_sensortriggered=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_nightring=yes"
Delete the "Enter PGROUP" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_enterpgroupl=yes"
Delete the "Invalid PGROUP" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_invalidpgroup=yes"
Delete the "Enter Code" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_entercode=yes"
Delete the "Invalid Code" audio file	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "delete_invalidcode=yes"
Trigger the Fault Detection Test (Fault Detection page)	wget --user admin --password admin --auth-no- challenge --quiet - O /dev/null "http://10.0.3.71/cgi- bin/sensorconfig.cgi" --post-data "intrusiontest=yes"

a.Type and enter all of each http POST command on one line.

Appendix A: Setting Up a TFTP Server

A.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

A.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   `in.tftpd -l -s /tftpboot/`*`your_directory_name`*

A.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solar Winds freeware TFTP server, which you can download at:

http://www.cyberdata.net/support/voip/solarwinds.html

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security** tab/**Transmit Only**.

Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

Go to the following URL to see CyberData's list of frequently asked questions:

http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/faqs.html

B.1.1 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation at:

http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/docs.html

B.2 Contact Information

Contact

CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.CyberData.net
Phone: 800-CYBERDATA (800-292-3732)
Fax: 831-373-4193

Sales

Sales 831-373-2601 Extension 334

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

http://www.cyberdata.net/support/contactsupportvoip.php

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net

Returned Materials Authorization

To return the product, contact the Returned Materials Authorization (RMA) department:

Phone: 831-373-2601, Extension 136
Email: RMA@CyberData.net

When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:

CyberData Corporation
3 Justin Court
Monterey, CA 93940
Attention: RMA "your RMA number"

RMA Status Form

If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:

http://www.cyberdata.net/support/rmastatus.html

B.3 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail Within Warranty, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail Out of the Warranty period, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are Within Warranty period but are damaged by improper installation, modification, or abuse are deemed Out of Warranty and will be charged at the Out of Warranty rate. A device is deemed Out of Warranty when its purchase date is longer than two years or when the device has been damaged due to human error during installation, modification, or abuse. A replacement unit will be offered at full cost if the device cannot be repaired.

End of Life Devices are included under this policy. End of Life devices are devices that are no longer produced or sold. Technical support is still available for these devices. However, no firmware revisions or updates will be provided. If an End of Life device cannot be repaired, the replacement offered may be the current version of the device.

Products shipped to CyberData, both within and out of warranty, are shipped at the expense of the customer. CyberData will pay return shipping charges for repaired products.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

B.3.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

B.3.2 Warranty & RMA Returns outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

B.3.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

http://www.cyberdata.net/support/warranty/spareintheair.html

B.3.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

B.3.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

http://www.cyberdata.net/support/warranty/index.html

Index

Symbols

+48V DC power supply 9

Numerics

100 Mbps indicator light 11

A

activity light 11
address, configuration login 15
addressing
    DHCP 13, 23
    static 13, 23
admin username and password 15
audio configuration 43
    night ring tone parameter 46
audio configuration page 43
audio ground reference 8
audio output 8
authenticate ID and password for SIP server registration 27
Autoprovision at time (HHMMSS) 57
autoprovision at time (HHMMSS) 57
autoprovision when idle (in minutes > 10) 57
autoprovisioning 57, 58
    autoprovisioned audio files 60
    autoprovisioned firmware upgrades 59
    autoprovisioning autoupdate 59
    autoprovisioning enabled option 58
    autoprovisioning from DHCP 58
    autoprovisioning server (IP address) 59
    get autoprovisioning template button 57
autoprovisioning autoupdate (in minutes) 57
autoprovisioning configuration 56, 57
autoprovisioning filename 57
autoprovisioning server (IP Address) 57

B

backup SIP server 1 26
backup SIP server 2 26
backup SIP servers, SIP server backups 26
beep on page setting 20

C

cat 5 ethernet cable 9
changing
    the web access password 19
changing default username and password for configuration GUI 15
Cisco SRST 26
command interface 69
commands 69
configurable parameters 17, 20, 23
configuration 17
    beep on page setting 20
configuration information 13
configuration page
    configurable parameters 17, 20, 23
connecting the V3 paging server 7
connection options 7
connection speed 11
    specification 4
    verifying 11
connections 7
connector (removable) 8
contact information 75
contact information for CyberData 75
Current Network Settings 23
current network settings 23
current settings, reviewing 18
CyberData contact information 75

D

default
    gateway 12
    IP address 12
    subnet mask 12
    username and password 12
default gateway 12, 23
default gateway for static addressing 24
default login address 15
default password for configuration GUI 15
default settings, restoring 12
default username and password for configuration GUI 15
device configuration 19
    beep on page setting 20
    device configuration parameters 57
    the device configuration page 56
device configuration page 19
device configuration parameters 20
device configuration password

changing for web configuration access 19
DHCP addressing 13, 23
DHCP IP addressing 23
dimensions 4
discovery utility program 15
DNS server 23
door sensor 46
download protocol, HTTP or TFTP 57

E

enable night ring events 52
ethernet port 9
event configuration
enable night ring events 52
expiration time for SIP server lease 26, 27, 30
export configuration button 17
export settings 17

F

fault sense input, sensor 8
features 3
firmware
where to get the latest firmware 67
firmware signature 65
firmware upgrade parameters 66
firmware, upgrade 65

G

get autoprovisioning from DHCP 57
get autoprovisioning template 57
get autoprovisioning template button 57
GMT table 63
GMT time 63
GUI username and password 15

H

hazard levels 6
http POST command 69

I

identifier names (PST, EDT, IST, MUT) 63
identifying your product 2
import configuration button 17
import settings 17
import/export settings 17
importing and exporting the device's configuration 17
input specifications 4
IP address 12, 23
SIP server 27
IP addressing 23
default
IP addressing setting 12

L

lease, SIP server expiration time 26, 27, 30
line input specifications 4
line output specifications 4
line-in 7
line-in to multicast setting
multicast, line-in to multicast setting
line-in, line-in to multicast setting 20
line-out 7
link light 11
Linux, setting up a TFTP server on 73
local SIP port 26, 27
log in address 15
logging in to configuration GUI 15

M

MGROUP 33
multicast 32
multicast address 32
multicast port 32
multicast TTL 41

N

navigation (web page) 14
navigation table 14
network activity, verifying 11
network configuration page 22
network parameters, configuring 22
network setup button 22
network, connecting to 10
Nightringer 29, 61
Nightringer in peer to peer mode (cannot be used) 29
nightringer settings 30
Nightringer, SIP registration required 29
NTP server 57

O

orange link LED 11
out of band 42
output specifications 4

P

page port 7
page port output connections 7
paging server
    configuration 13
part number 4
parts list 5
password
    configuration GUI 13, 15
    for SIP server login 26
    restoring the default 12
    SIP server authentication 27
pgroups 33
pin descriptions and functions 8
play audio via multicast 32
point-to-point configuration 28
port
    ethernet 9
    local SIP 26, 27
    remote SIP 26, 27
posix timezone string
    timezone string 57
POST command 69
power
    connecting to 9
    requirement 4
product overview 1

R

reboot 66, 68
    unregistering from SIP server during 27
registration and expiration, SIP server
    lease expiration 27
regulatory compliance 4
relay 8
relay contact 8
remote SIP port 26, 27
required configuration for web access username and password 13, 15
resetting the IP address to the default 74
restoring factory default settings 12
return and restocking policy 77
RFC2833 RTP events 42
RMA returned materials authorization 75
RMA status 75

S

safety instructions 5
sales 75
server
    TFTP 73
server address, SIP 26
service 75
set the time from the NTP server 57
set time with external NTP server on boot 57
SIP
    enable SIP operation 26
    local SIP port 26
    user ID 26
SIP configuration
    SIP Server 26
SIP configuration page 25
SIP configuration parameters 26
    outbound proxy 26
    registration and expiration, SIP server lease 26, 30
    unregister on reboot 26
    user ID, SIP 26
SIP registration 26
SIP remote SIP port 26
SIP server 26
    password for login 26
    unregister from 26
    user ID for login 26
SIP server parameters, configuring 13
SIP settings 26, 27
SIP setup button 25
Spare in the Air Policy 77
specifications 4
SRST 26
static addressing 13, 23
static IP addressing 23
status light 11
Stored Network Settings 23
subnet mask 12, 23
subnet mask static addressing 24
supported protocols 4

T

tech support 75
technical support, contact information 75
TFTP server 73
time zone string examples 63

U

unregister from SIP server 27
upgrade firmware 65
user ID
    for SIP server login 26
user ID for SIP server registration 27
username
    changing for web configuration access 19
    restoring the default 12
username for configuration GUI 13, 15

V

verifying
    connection speed 11
    network activity 11
    network connectivity 11
VLAN ID 23
VLAN Priority 23
VLAN tagging support 23
VLAN tags 23

W

warranty 76
warranty & RMA returns outside of the United States 76
warranty and RMA returns page 77
warranty policy at CyberData 76
web access password 12
web access username 12
web configuration log in address 15
web page
    navigation 14
web page navigation 14
weight 4
wget, free unix utility 69
Windows, setting up a TFTP server on 73